REPRESENTATIONS OF FINITE GROUPS

This is a preliminary version of a revised version of the chapter on group representations. I don't want to include it yet in the full course notes because some of you may have been using the current version of the notes and the switch to a new version may be confusing.

The notes below follow the presentation of the material as we have done it this year in class. There are probably typos, hopefully all self-evident and easily fixable. However, if you note any typos, I will be grateful if you let me know.

– Eyal Goren

Contents

1. Representations of finite groups

In this chapter, we only consider finite groups G and finite dimensional complex vector spaces V. The theory of representations of infinite groups and infinite-dimensional representations is vast, and important, but is too advanced for this course. We should mention that even if one is interested in representation of Lie groups, which arise often in physics, for example the groups $\mathrm{GL}_n(\mathbb{C}), U_n(\mathbb{C})$, the theory of representations of finite groups plays an important role.

Group representations are intimately related to understanding how groups acts on sets. In our current setting, the set is a complex vector space and the group acts through very particular symmetries – invertible linear transformations. Thus, this topic can be viewed as a natural continuation of our study of groups actions.

Group representations are a subject with many applications to other branches of mathematics, and outside mathematics, for example for computer science, physics, chemistry, and electrical engineering. We will see some of those at the end of this chapter. It is also a topic that is a beautiful marriage of linear algebra and group theory, thus connecting two courses that are usually not taken together.

1.1. First definitions.

A **linear representation** of a (finite) group G is a homomorphism

$$\rho\colon G \to \mathrm{GL}(V) := \{T\colon V \to V : T \text{ is an invertible linear transformation}\},$$

where V is a finite dimensional complex vector space. We will usually drop the adjective "linear". We note that $\mathrm{GL}(V)$ is a group under composition of linear maps. We will denote such a representation by (ρ, V), where the group G is understood from the context. When we feel confident enough, we may just denote it ρ, or V, depending which notation seems more useful at that point.

A very important notion is when are two representations isomorphic. Given two representations (ρ_i, V_i) of G we define

$$\mathrm{Hom}_G(V_1, V_2) = \{T\colon V_1 \to V_2 \text{ linear} : T \circ \rho_1(g) = \rho_2(g) \circ T, \forall g \in G\}.$$

We note that there is no assumption that T is invertible, or even that $\dim(V_1) = \dim(V_2)$; in particular, we always have that the zero map is an element of $\mathrm{Hom}_G(V_1, V_2)$. Further, under addition of linear maps and multiplication by a scalar, $\mathrm{Hom}_G(V_1, V_2)$ is a complex vector space. We shall refer to elements of it as **homomorphisms of representations**, or **G-homomorphisms**.

Having made this definition, the notion of an **isomorphism** $(\rho_1, V_1) \cong (\rho_2, V_2)$ is clear: these are linear maps $T \in \mathrm{Hom}_G(V_1, V_2)$ that are invertible. In that case, the inverse map always satisfies $T^{-1} \in \mathrm{Hom}_G(V_2, V_1)$.

Main Goal: Classify representations of G up to isomorphism.

(We will make this more precise later on).

Given a representation (ρ, V), *choose* an isomorphism $T\colon V \to \mathbb{C}^n$ ($n = \dim(V)$) and let

$$\tau\colon G \to \mathrm{GL}(\mathbb{C}^n), \quad \tau(g) = T \circ \rho(g) \circ T^{-1}.$$

It is easily verified that

$$(\rho, V) \cong (\tau, \mathbb{C}^n),$$

where the isomorphism is the map T itself. Therefore, every isomorphism class of representations is represented by some $(\tau, \mathbb{C}^n)$. How unique is τ? It is unique up to conjugation by elements of $\mathrm{GL}(\mathbb{C}^n)$: for any $T_1 \in \mathrm{GL}(\mathbb{C}^n)$ we have

$$\tau \cong \tau_1,$$

where

$$\tau_1(g) = T_1 \circ \tau(g) \circ T_1^{-1}.$$

(this reflects the fact that we had to choose an isomorphism $T\colon V \to \mathbb{C}^n$ and the freedom in this choice is precisely modifying T to $T_1 \circ T$).

It follows that we can make everything more concrete by using the natural identification

$$\mathrm{GL}(\mathbb{C}^n) = \mathrm{GL}_n(\mathbb{C}),$$

obtained by representing any linear transformation T by its matrix $[T]$ relative to the usual basis of $\mathbb{C}^n$. Thus, we may think about a representation also as a homomorphism

$$\tau\colon G \to \mathrm{GL}_n(\mathbb{C}).$$

The homomorphism rule is $\tau(xy) = \tau(x)\tau(y)$, where on the right we find matrix multiplication.

When do two such homomorphisms define isomorphic representations? For any invertible matrix $M \in \mathrm{GL}_n(\mathbb{C})$, we have

$$\tau \cong \rho, \qquad \rho(g) = M\tau(g)M^{-1}, \forall g \in G,$$

and conversely. This may be a confusing point, so let's repeat it: we are allowed to choose any matrix $M \in \mathrm{GL}_n(\mathbb{C})$, but once we made the choice the relation $\rho(g) = M\tau(g)M^{-1}$ should hold for all $g \in G$ with the same M.

Although we arrived finally at a rather concrete model for representations, the general point of view $\rho\colon G \to \mathrm{GL}(V)$ is very useful as often the vector space V doesn't have a natural basis.

We now come to one of the key notions of this whole subject: the character of a representation. Given a representation

$$\rho\colon G \to \mathrm{GL}(V),$$

we define its **character** χ_ρ as follows:

$$\chi_\rho\colon G \to \mathbb{C}, \quad \chi_\rho(g) = \mathrm{Tr}(\rho(g)).$$

It is important to note that χ_ρ is simply a function; it associate to each element g the trace of the linear operator $\rho(g)$. Usually it will not have any multiplicative properties.

The notion of a character will turn out to be central for the whole theory and we will study many properties of characters. For now, we only give a few basic facts.

Lemma 1.1.1. *(1) χ_ρ only depends on the isomorphism class of ρ.*

(2) χ_ρ is constant on conjugacy classes in G.

(3) $\chi(1) = \dim(V)$.

Proof. To calculate the trace of an operator $\rho(g)$ one needs to choose a basis B for V and represent $\rho(g)$ by a matrix $[\rho(g)]_B$. If we choose another basis, say C, then the matrices of $\rho(g)$ in the two bases are related by

$$[\rho(g)]_C = M[\rho(g)]_B M^{-1},$$

where M is the change of basis matrix. Note that if we pass from ρ to an isomorphic representation, say (τ, W),

$$\tau(g) = T\rho(g)T^{-1}$$

then once more

$$[\tau(g)]_C = M[\rho(g)]_B M^{-1},$$

where now C is a basis of W and M is the matrix representing T relative to the two bases B, C. Thus, in both cases, we have to show that

$$\mathrm{Tr}(M[\rho(g)]_B M^{-1}) = \mathrm{Tr}([\rho(g)]_B).$$

This is well known (it follows from the formula $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ that one proves by writing down the product of the matrices explicitly and calculating the trace).

The proof that χ_ρ is constant on conjugacy classes is very similar. Relative to some basis B we have

$$\mathrm{Tr}([\rho(hgh^{-1})]_B) = \mathrm{Tr}([\rho(h)\rho(g)\rho(h)^{-1}]_B) = \mathrm{Tr}([\rho(h)]_B[\rho(g)]_B[\rho(h)^{-1}]_B) = \mathrm{Tr}([\rho(g)]_B).$$

Finally, we have $\chi_\rho(1_G) = \mathrm{Tr}(\mathrm{Id}_V) = \mathrm{Tr}(I_{\dim(V)}) = \dim(V)$, where we denote by Id_V the identity operator on V and by I_d the $d \times d$ identity matrix. □

2. Examples

We now discuss some relatively simple examples. Despite appearances, perhaps, they will turn out to be very important and will make frequent appearances. Study them carefully!

2.1. 1-dimensional representations.

A 1-dimensional representation of G could be thought of simply as a homomorphism

$$\rho\colon G \to \mathbb{C}^\times.$$

Indeed, $\mathrm{GL}_1(\mathbb{C}^\times) = \mathbb{C}^\times$. Note that in this case if $\rho \cong \tau$ then, since $\mathbb{C}^\times$ is commutative, we actually have $\rho = \tau$. Also, since the trace of a 1×1 matrix is (α) is just α it follows that

$$\chi_\rho = \rho.$$

For these reasons, 1-dimensional representations are also called **1-dimensional characters**, or **multiplicative characters** .

Let

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times).$$

We make two observations: First, G^* is a group under the rule

$$(\rho \cdot \tau)(g) = \rho(g) \cdot \tau(g).$$

Second, if we let $S^1 = \{z \in \mathbb{C}^\times : |z| = 1\}$ denote the unit circle in $\mathbb{C}$ then

$$G^* = \mathrm{Hom}(G, S^1).$$

Indeed, if $g \in G$ is of order d, $\rho \in G^*$, then $\rho(g)^d = \rho(1_G) = 1$ which implies that $\rho(g)$ is necessarily a root of unity. The group G^* is called the **character group** of G.

Lemma 2.1.1. *There is a natural isomorphism*

$$G^* \cong (G^{ab})^*,$$

where, as usual, $G^{ab} = G/G'$ is the abelianization of G.

Proof. We have seen that any homomorphism $G \to A$, where A is an abelian group, factors uniquely through G^{ab} (see **??**). In particular, given any homomorphism $f\colon G \to \mathbb{C}^\times$ there is a unique homomorphism $F\colon G^{ab} \to \mathbb{C}^\times$ such that the following diagram commutes (π being the natural map $G \to G/G'$):

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & \mathbb{C}^\times \\ & G^{ab} \arrow[ur, "F"'] & \end{tikzcd} ,$$

and conversely. □

We will revisit this example later on. We will rely on Exercise **??** that you are encouraged to do at this point.

Example 2.1.2. The alternating groups A_n for $n \geq 5$ have only one 1-dimensional representation, which is the trivial representation $\mathbb{1}$. For any group G the **trivial representation** $\mathbb{1}$ is the 1-dimensional representation

$$G \to \mathbb{C}^\times, \quad g \mapsto 1, \forall g \in G.$$

Its character, also denoted $\mathbb{1}$, is the constant function 1.

The symmetric groups S_n, for $n \geq 5$, have only two 1-dimensional characters, $\mathbb{1}$ and sgn. Indeed, the only non-trivial normal subgroup of S_n, for $n \geq 5$, is A_n and, as $S_n/A_n \cong \{\pm 1\}$ is abelian, it must be that $S_n^{ab} \cong \{\pm 1\}$. The group $\{\pm 1\}$ has precisely two homomorphisms to $\mathbb{C}^\times$, the trivial one and the identity one.

Example 2.1.3. The commutator subgroup of D_4 is $\{1, x^2\}$. Indeed, $[x, y] = x^2$ and so the commutator subgroup contains $\langle x^2 \rangle$. On the other hand, x^2 commutes with x and y and is therefore a central element and thus $\langle x^2 \rangle$ is a normal subgroup. As $D_4/\langle x^2 \rangle$ has order 2^2 it is abelian and it follows that $\langle x^2 \rangle \supseteq D_4'$ and we get equality: $D_4' = \langle x^2 \rangle$. We think about the abelianization as

$$D_4^{ab} = \{1, \bar{x}, \bar{y}, \overline{xy}\}$$

with $\bar{x}\bar{y} = \bar{y}\bar{x}$ and the square of every element is 1; it is a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. As every element has order 2, every multiplicative character of D_4^{ab} takes values in $\{\pm 1\}$. It is not hard to show that there are 4 possibilities as described in the following table.

	1	$\bar{x}$	$\bar{y}$	$\overline{xy}$
$\rho_1 = \mathbb{1}$	1	1	1	1
ρ_2	1	-1	1	-1
ρ_3	1	1	-1	-1
ρ_4	1	-1	-1	1

2.2. **The regular representation ρ^{reg}.** Let G be a group. We define a vector space V with a basis $\{e_g : g \in G\}$. Often V is called the **group ring** of G and denoted $\mathbb{C}[G]$. A vector in V is a sum

$$\sum_{g \in G} a_g \cdot e_g,$$

with a_g complex numbers. We can also think about V as

$$\{\sum_{g \in G} a_g \cdot [g] : a_g \in \mathbb{C}\}.$$

The two notations are equivalent – the symbol $[g]$ corresponds to the notation e_g. In the second notation, we can see that $\mathbb{C}[G]$ has a ring structure, where

$$(\sum_{g\in G} a_g \cdot [g]) + (\sum_{g\in G} a_g \cdot [g]) = \sum_{g\in G} (a_g + b_g) \cdot [g],$$

and

$$(\sum_{g\in G} a_g \cdot [g])(\sum_{g\in G} b_g \cdot [g]) = \sum_{g\in G} (\sum_{s\in G} a_{gs^{-1}} b_s) \cdot [g].$$

However, the ring structure will not be important until much later.

The group G acts on this vector space and this representation is called the **regular representation** and denoted ρ^{reg}. We have

$$\rho^{reg} \colon G \to \mathrm{GL}(V), \qquad \rho^{reg}(g)(e_h) = e_{gh}, \ \forall g, h \in G.$$

In the other notation,

$$\rho^{reg}(g)(\sum_{s\in G} a_s[s]) = [g](\sum_{s\in G} a_s[s]) = \sum_{s\in G} a_s[gs].$$

The character χ^{reg} of ρ^{reg} is very simple:

$$\chi^{reg}(g) = \begin{cases} \sharp G, & g = 1_g; \\ 0, & else. \end{cases} \tag{1}$$

The proof is simple: if $\{e_1, \dots, e_n\}$ is a basis for a vector space W, and $T \colon W \to W$ is a linear transformation, write

$$T(e_i) = \sum_{a=1}^{n} b_a e_a, \ b_a \in \mathbb{C}.$$

Then, the contribution to $\mathrm{Tr}(T)$ from the vector e_i is b_i. Now, to calculate $\mathrm{Tr}(\rho^{reg}(g))$ we see that the contribution from the vector e_h is the coefficient of e_h in $\rho^{reg}(g)(e_h)$. As $\rho^{reg}(g)(e_h) = e_{gh}$, this contribution is 0 from *every* h if $g \neq 1$, and is 1 from every h if $g = 1$.

2.3. **Direct sum.** Let (ρ, V_1), (ρ_2, V_2) be two representations of the group G. We define the **direct sum** of the representations: the vector space is $V_1 \oplus V_2$ and

$$\rho_1 \oplus \rho_2 \colon G \to \mathrm{GL}(V_1 \oplus V_2), \quad (\rho_1 \oplus \rho_2)(g)(v_1, v_2) := (\rho_1(g)(v_1), \rho_2(g)(v_2)).$$

If we represent ρ_i as homomorphisms,

$$\rho_i \colon G \to \mathrm{GL}_{n_i}(\mathbb{C}) \quad (n_i = \dim(V_i)),$$

then

$$\rho_1 \oplus \rho_2 \colon G \to \mathrm{GL}_{n_1+n_2}(\mathbb{C}), \quad (\rho_1 \oplus \rho_2)(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

It is then clear that

$$\chi_{\rho_1 \oplus \rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g).$$

3. Subrepresentations and irreducible representations

3.1. **Subrepresentions.** Let (ρ, V) be a representation of G. Let $U \subseteq V$ be a subspace such that

$$\rho(g)(u) \in U, \quad \forall g \in G, \forall u \in U.$$

That is, U is invariant under all the linear maps $\{\rho(g) : g \in G\}$. Then U is called a **subrepresentation** of V; we have

$$\rho|_U \colon G \to \mathrm{GL}(U), \quad \rho|_U(g) := \rho(g)|_U.$$

Example 3.1.1. $\{0\}$ and V are always sub-representations. We refer to them as **trivial subrepresentations.**

Example 3.1.2. The **standard representation** ρ^{std} of S_n.

Let $n \geq 2$. We consider S_n as contained in $\mathrm{GL}_n(\mathbb{C})$ in such a way that

$$\sigma(e_i) = e_{\sigma(i)}, \quad i = 1, 2, \dots, n.$$

This is called the standard n-dimensional representation of S_n. For example, for $n = 3$,

$$(12) \leftrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \leftrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Let χ^{std} be the character of ρ^{std}. In our example of $n = 3$ we have $\chi^{std}(12) = 1, \chi^{std}(123) = 0$.

Proposition 3.1.3. *We have*

$$\chi^{std}(\sigma) = \sharp \text{ fixed points of } \sigma. \tag{2}$$

Proof. The contribution to $\mathrm{Tr}(\rho^{std}(\sigma))$ coming from the basis vector e_i is the coefficient of e_i in $\rho^{std}(\sigma)(e_i) = e_{\sigma(i)}$, which is 1 is $\sigma(i) = i$ and 0 if $\sigma(i) \neq i$. Summing over all i, we find the statement in the proposition. □

Consider now the subspaces

$$U_1 := \{(a, \dots, a) : a \in \mathbb{C}\},$$

and

$$U_0 := \{(x_1, \dots, x_n) : \sum_{i=1}^n x_i = 0, x_i \in \mathbb{C}\}.$$

The space U_1 is just the trivial representation $\mathbb{1}$ of S_n, and U_0 is also a representation of S_n that we denote $\rho^{std,0}$. As $\dim(U_1) + \dim(U_0) = n$ and $U_1 \cap U_0 = \{0\}$, we find:

$$\rho^{std} = \mathbb{1} \oplus \rho^{std,0}.$$

3.2. **Irreducible representations and Maschke's Theorem.** A representation (ρ, V) of G is called **irreducible** if its only subrepresentations are $\{0\}$ and V, and $V \neq 0$.

Proposition 3.2.1. *The representations $\mathbb{1}$ and $\rho^{std,0}$ are irreducible representations of S_n. Thus, we have a decomposition of ρ^{std} as a sum of irreducible representations.*

Proof. Clearly $\mathbb{1}$ is irreducible for dimension reasons – there aren't any non-trivial subspaces; this is true for any group G and any 1-dimensional representation of it.

The proof for U_0 is slightly involved; we will give another proof later, much more elegant, as an application of character theory.

We assume that $n > 2$. The case $n = 2$ is easy as U_0 is 1-dimensional.

Let $U' \subseteq U_0$ be a non-zero sub-representation. Let $x = (x_1, \dots, x_n)$ be a non-zero vector in U'. If x has precisely two zero elements, by multiplying x by a scalar we may assume that

$x = (0, \dots, 0, 1, 0 \dots, 0, -1, 0, \dots, 0)$. Then, by acting by S_n we see that every vector of the form $e_i - e_j$ (where e_i are the standard basis) is also in U'. But these vectors span U_0 and it follows that $U' = U_0$.

Thus, it remains to prove that U' always contains such a vector. Let $x \in U'$ be a non-zero vector. If x has more than 2 non-zero coordinates, we show that there is vector $y \in U'$ that is not zero and has fewer non-zero coordinates. This suffices to reduce to the case considered above.

Assume therefore that x has at least 3 non-zero coordinates. First, by rescaling we may assume that one of these coordinates is 1. Then, as $\sum x_i = 0$, there exists a non-zero coordinate that is not equal to 1. By applying a permutation to x we may assume that

$$x = (1, x_2, x_3, \dots, x_n),$$

where $x_2 \neq 1$ and is non-zero and also $x_3 \neq 0$. In this case, also the vector

$$x' = \frac{1}{x_2}(x_2, 1, x_3, \dots, x_n),$$

belongs to U_1. Therefore, also

$$y = x - x' = (0, x_2 - \frac{1}{x_2}, x_3(1 - \frac{1}{x_2}), \dots, x_n(1 - \frac{1}{x_2})),$$

belongs to U' and this vector has fewer non-zero coordinates, yet is not zero (consider its third coordinate). □

Theorem 3.2.2 (Maschke). *Every non-zero representation (ρ, V) decomposes as a direct sum of irreducible representations.*

Remark 3.2.3. We will later prove that such a direct sum decomposition is unique, up to isomorphism and re-ordering of the summands. We can now make our goal in this chapter more precise:

Goal. Classify the irreducible representations of a group G. Find effective methods to determine the decomposition of a representation into irreducible representations.

Proof. (Maschke's Theorem) We begin with a lemma that shows that we can always define an inner product of V relative to which $\rho(g)$ is a unitary matrix for any $g \in G$.

Lemma 3.2.4. *There is an inner product*

$$\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C},$$

such that

$$\langle gv, gu \rangle = \langle u, v \rangle, \forall g \in G, \forall u, v \in V.$$

(To simplify notation we write gv for $\rho(g)(v)$.)

Proof. (Lemma) Let $(\cdot, \cdot)$ be *any* inner product on V. Define,

$$\langle v, u \rangle = \frac{1}{\sharp G} \sum_{g \in G} (gv, gu).$$

The verification that this is an inner product is straightforward and we omit it. To check that ρ is a unitary representation relative to this inner product we calculate:

$$\begin{aligned}\langle gv, gu\rangle &= \frac{1}{\sharp G}\sum_{h\in G}(hgv, hgu)\\ &= \frac{1}{\sharp G}\sum_{h\in G}(hv, hu)\\ &= \langle v, u\rangle,\end{aligned}$$

where we used that when h runs over G so does hg. □

We now get to the proof of the theorem. We prove it by induction on $\dim(V)$.

If $\dim(V) = 1$ then V is irreducible and there is nothing to prove. In general, if V is irreducible there is nothing to prove. Otherwise, V has a subrepresentation $0 \neq U \neq V$. Let $\langle v, u\rangle$ be a G-invariant inner product on V, as in the Lemma. Then

$$V = U \oplus U^\perp.$$

We only need to show that

$$U^\perp := \{v \in V : \langle v, u\rangle = 0, \forall u \in U\}$$

is a subrepresentation. Let $g \in G$ and $v \in U^\perp$. For any $u \in U$ we have

$$\langle gv, u\rangle = \langle v, g^{-1}u\rangle = 0,$$

because $g^{-1}u \in U$ as U is a subrepresentation. It follows that $gv \in U^\perp$.

By induction,

$$U = W_1 \oplus \cdots \oplus W_a, \quad U^\perp = W_{a+1} \oplus \cdots \oplus W_b,$$

for some irreducible representations W_i of G. Then,

$$V = U \oplus U^\perp = W_1 \oplus \cdots \oplus W_b$$

is a sum of irreducible representations too. □

3.3. **The projection on V^G.** Let (ρ, V) be a representation of G. Let

$$V^G = \{v \in V : \rho(g)(v) = v, \forall g \in G\}.$$

Then V^G is a subrepresentation on which G acts trivially. It's the space of **invariant vectors**.

Lemma 3.3.1. *Let*

$$\pi(v) = \frac{1}{\sharp G}\sum_{g\in G}\rho(g)(v). \tag{3}$$

Then $\pi \in \mathrm{Hom}_G(V, V^G)$ and is a projection on the subspace V^G.

Proof. As π is a sum of linear maps it is certainly a linear map from V to V. We first show that $\mathrm{Im}(\pi) \subseteq V^G$. We need to show that all $h \in G, v \in V$ we have $\rho(h)(\pi(v)) = \pi(v)$. Indeed, $\rho(h)(\pi(v)) = \frac{1}{\sharp G}\sum_g(\rho(h)\circ\rho(g))(v) = \frac{1}{\sharp G}\sum_g \rho(hg)(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \pi(v)$.

To show π is a projection, we need to verify that π is the identity on V^G. But, for $v \in V^G$ we have $\pi(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \frac{1}{\sharp G}\sum_g v = v$.

Finally, we check that π is a homomorphism of representations. As G acts trivially on V^G this boils down to verifying that $\pi(\rho(h)v) = \pi(v)$. We calculate: $\pi(\rho(h)(v)) = \frac{1}{\sharp G}\sum_g \rho(g)(\rho(h)v) = \frac{1}{\sharp G}\sum_g \rho(gh)(v) = \frac{1}{\sharp G}\sum_g \rho(g)(v) = \pi(v)$. □

The following corollary will be used several times in the sequel:

Corollary 3.3.2 (Projection Formula)**.** *We have*

$$\dim(V^G) = \frac{1}{\sharp G}\sum_g \chi_\rho(g). \tag{4}$$

In words, the dimension of the subspace of invariant vectors is the average value of the character χ_ρ.

Proof. We have a decomposition,

$$V = V^G \oplus \mathrm{Ker}(\pi).$$

In this decomposition we can write

$$\pi = \mathrm{Id}_{V^G} \oplus 0.$$

Thus, $\mathrm{Tr}(\pi) = \dim(V^G)$. But on the other hand,

$$\mathrm{Tr}(\pi) = \frac{1}{\sharp G}\sum_g \mathrm{Tr}(\rho(g)) = \frac{1}{\sharp G}\sum_g \chi_\rho(g).$$

□

4. Schur's lemma and orthogonality of characters

4.1. **The dual representation and the two Homs.** Let (ρ, V) be a representation of G. For any linear operator $\rho(g)\colon V \to V$ we have the dual operator $\rho(g)^t\colon V^* \to V^*$, where $V^* = \mathrm{Hom}(V, \mathbb{C})$ is the dual vector space to V. Recall that $\rho(g)^t$ is defined by

$$\rho(g)^t(\phi) = \phi \circ \rho(g), \quad \phi \in V^*.$$

Further, if $\{e_1, \dots, e_n\}$ are a basis for V and $\{\phi_1, \dots, \phi_n\}$ is the dual basis for V (the basis that satisfies $\phi_i(e_j) = \delta_{ij}$) then in terms of matrices we have

$$[\rho(g)^t]_{\{\phi_i\}} = ([\rho(g)]_{\{e_i\}})^t.$$

Define the **dual representation** ρ^*

$$\rho^*\colon G \to \mathrm{GL}(V^*), \quad \rho^*(g) = (\rho(g^{-1}))^t.$$

Proposition 4.1.1. *ρ^* is a representation of G and its character satisfies $\chi_{\rho^*} = \bar{\chi}_\rho$. That is,*

$$\chi_{\rho^*}(g) = \overline{\chi}_\rho(g) := \overline{\chi_\rho(g)}, \ \ \forall g \in G.$$

Proof. The proof is easy, but reveals two properties that are very important, and general, and so we record them here as a lemma.

Lemma 4.1.2. *Let (ρ, V) be a representation of G. Then:*

(1) Every $\rho(g)$ is diagonalizable.
(2) Every eigenvalue of $\rho(g)$ is a root of unity of order dividing d, where d is the order of g in G.

Proof. Let d be the order of g. As ρ is a homomorphism $\rho(g)^d = \rho(g^d) = \rho(1_G) = \mathrm{Id}_V$. It follows that $\rho(g)$ solves the polynomial $x^d - 1$, which is a separable polynomial (i.e., it has distinct roots over $\mathbb{C}$). Therefore, also the minimal polynomial of $\rho(g)$ is a separable polynomial and, consequently, $\rho(g)$ is diagonalizable. Let's write

$$\rho(g) \sim \mathrm{diag}(\alpha_1, \dots, \alpha_n),$$

where $n = \dim(V)$ and α_i are d-th roots of unity. □

Note that in general the basis in which $\rho(g)$ is diagonal depends on g; we cannot, in general, diagonalize all $\rho(g)$ simultaneously. However, $\rho(g^{-1}) = \rho(g)^{-1}$ is given in the same basis by

$$\mathrm{diag}(\alpha_1^{-1}, \dots, \alpha_n^{-1}) = \mathrm{diag}(\overline{\alpha_1}, \dots, \overline{\alpha_n}),$$

because the α_i are roots of unity. Thus,

$$\chi_\rho(g^{-1}) = \sum_i \overline{\alpha_i} = \overline{\chi_\rho(g)}. \tag{5}$$

To finish the proof of the Proposition it only remains to check that ρ^* is a representation. We have:

$$\rho^*(gh) = (\rho(gh)^{-1})^t = (\rho(h^{-1})\rho(g^{-1}))^t = (\rho(g^{-1}))^t \cdot (\rho(h^{-1}))^t = \rho^*(g) \cdot \rho^*(h).$$

□

We now discuss "the two Homs" and engage in a very technical calculation. However, the results will be absolutely essential to proving one of the most important theorems concerning representations: orthogonality of characters.

Let $(\rho, V), (\tau, W)$ be two representations of the group G. We have already defined (all maps appearing below are understood to be linear)

$$\mathrm{Hom}_G(V, W) = \{T \colon V \to W : T \circ \rho(g) = \tau(g) \circ T, \forall g \in G\}.$$

We also have the more naive

$$\mathrm{Hom}(V, W) = \{T \colon V \to W\}.$$

Proposition 4.1.3. $\mathrm{Hom}_G(V, W)$ *is a linear representation* σ *of* G*, where*

$$\sigma(g)(T) = \tau(g) \circ T \circ \rho(g)^{-1}, \quad T \in \mathrm{Hom}(V, W).$$

Remark 4.1.4. Note the following:

1. $\dim(\mathrm{Hom}(V, W)) = \dim(V) \cdot \dim(W)$. This can be seen by choosing bases for the two vector spaces and representing the linear maps as matrices. See also the proof for the character formula below.
2. We have the following relationship between the two Homs:
$$\mathrm{Hom}_G(V, W) = \mathrm{Hom}(V, W)^G.$$
3. Consider the special case where $(\tau, W) = (\mathbb{1}, \mathbb{C})$. In this case
$$\mathrm{Hom}(V, W) = V^*,$$
and the new representation σ we have now defined on it is:
$$\sigma(g)(\phi) = \tau(g) \circ \phi \circ \rho(g^{-1}) = \phi \circ \rho(g^{-1}) = \rho(g^{-1})^t(\phi) = \rho^*(\phi).$$
Namely, we just get the dual representation again.

Proof. There is actually quite a bit to verify here. We only indicate what should be verified and leave the verification as an exercise.

- As $\mathrm{Hom}(V, W)$ is a complex vector space, we need to verify that for every $g \in G$, $\sigma(g)$ is an endomorphism of that space. Namely, that indeed $\tau(g) \circ T \circ \rho(g^{-1})$ is a linear map from V to W, and that
$$T \mapsto \tau(g) \circ T \circ \rho(g^{-1}),$$
is linear in T. This just establishes that $\sigma(g)$ is a linear map from the vector space $\mathrm{Hom}(V, W)$ to itself.

- Next, one needs to verify that $\sigma(gh) = \sigma(g) \circ \sigma(h)$. This shows that we have a multiplicative map $G \to \mathrm{End}(\mathrm{Hom}(V, W))$. But note that since every element in G is invertible and $\sigma(1)$ is the identity map, automatically $\sigma(g)$ is invertible (because $\sigma(g) \circ \sigma(g^{-1}) = \sigma(1) = \mathrm{Id}$, etc.). Thus, it follows that we get a homomorphism
$$\sigma : G \to \mathrm{GL}(\mathrm{Hom}(V, W)).$$

□

Theorem 4.1.5. *The character χ_σ of the representation $(\sigma, \mathrm{Hom}(V, W))$ is given by the formula*
$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

Proof. We first find a convenient basis for $\mathrm{Hom}(V, W)$. Let
$$\mathscr{B} = \{e_1, \dots, e_n\}, \quad \mathscr{C} = \{f_1, \dots, f_m\},$$
be bases for V and W, respectively. Let
$$\mathscr{B}^* = \{e_1^*, \dots, e_n^*\},$$
be the dual basis for V^*. So, $e_i^*(e_j) = \delta_{ij}$ (Kronecker's delta).

We introduce the following notation: for $\phi \in V^*$ and $w \in W$, we let the symbol[1]
$$\phi \otimes w$$
denote the element of $\mathrm{Hom}(V, W)$ given by
$$v \mapsto \phi(v) \cdot w.$$
We quickly check that it is indeed a linear map: We have $(\phi \otimes w)(\alpha_1 v_1 + \alpha_2 v_2) = \phi(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = (\alpha_1 \phi(v_1) + \alpha_2 \phi(v_2)) \cdot w = \alpha_1 \phi(v_1) \cdot w + \alpha_2 \phi(v_2) \cdot w = \alpha_1 \cdot (\phi \otimes w)(v_1) + \alpha_2 \cdot (\phi \otimes w)(v_2)$.

In particular, we have the maps $e_i^* \otimes f_j$. It turns out that these maps have very simple representation as matrices. Using the bases $\mathscr{B}, \mathscr{C}$, we have an identification
$$\mathrm{Hom}(V, W) \cong M_{m \times n}(\mathbb{C}),$$
by sending any linear transformation to its matrix representation relative to these bases. Since we have $(e_i^* \otimes f_j)(e_\ell) = \delta_{i\ell} f_j$, it follows that $e_i^* \otimes f_j$ is represented by the elementary matrix E_{ij} that has all entries equal to zero, except for the ij entry that is equal to 1:
$$e_i^* \otimes f_j \leftrightarrow E_{ij}.$$
As every matrix $(m_{ij}) \in M_{m \times n}(\mathbb{C}) \cong \mathrm{Hom}(V, W)$ is equal to $\sum_{ij} m_{ij} E_{ij}$, we find:

<u>Conclusion:</u> $\{e_i^* \otimes f_j : 1 \le i \le n, 1 \le j \le m\}$ is a basis for $\mathrm{Hom}(V, W)$.

We can calculate $\mathrm{Tr}(\sigma(g))$ by finding the action of $\sigma(g)$ on this basis. Let us introduce notation:
$$\tau(g) = (h_{ij})_{i,j=1}^m, \quad \rho(g^{-1}) = (g_{ij})_{i,j=1}^n.$$
Then,
$$\sigma(g)(e_j^* \otimes f_i) = (h_{ij}) E_{ij} (g_{ij}) = \begin{pmatrix} h_{11} & \dots & h_{1m} \\ \dots & \dots & \dots \\ h_{m1} & \dots & h_{mm} \end{pmatrix} \begin{pmatrix} 0 & \dots & 0 \\ g_{j1} & \dots & g_{jn} \\ 0 & \dots & 0 \end{pmatrix} = (r_{ab}).$$
The matrix on the right has all entries equal to zero except for its i-th row, which is equal to $(g_{j1}, g_{j2}, \dots, g_{jn})$. The result is a matrix (r_{ab}) whose ab entry is
$$r_{ab} = h_{ai} g_{jb}.$$

[1] The choice of notation is not accidental. There is a theory of tensor products that operates in the background, but we will not discuss it in this course.

In particular,

$$r_{ij} = h_{ii}g_{jj}.$$

Namely, we have

$$\sigma(g)(E_{ij}) = \sum_{a,b} h_{ai}g_{jb}E_{ab}.$$

The contribution to the trace of $\sigma(g)$ coming from the basis vector $e_j^* \otimes f_i = E_{ij}$ is $h_{ii}g_{jj}$. Thus,

$$\mathrm{Tr}(\sigma(g)) = \sum_{i,j} h_{ii}g_{jj} = (\sum_i h_{ii})(\sum_j g_{jj}) = \mathrm{Tr}(\tau(g)) \cdot \mathrm{Tr}(\rho(g^{-1})).$$

But, we have seen that $\mathrm{Tr}(\rho(g^{-1})) = \chi_\rho(g^{-1}) = \overline{\chi_\rho}(g)$. Therefore, we conclude that

$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

□

4.2. **Schur's Lemma.** Before proving Schur's lemma, we establish some general properties of homomorphisms of representations.

Lemma 4.2.1. *For any two representations $(\rho, V), (\tau, W)$ of G and any $T \in \mathrm{Hom}_G(V, W)$ we have that* $\mathrm{Ker}(T)$ *is a subrepresentation of V, and* $\mathrm{Im}(T)$ *is a subrepresentation of W.*

Proof. Let $v \in \mathrm{Ker}(T)$ and $g \in G$. We have

$$T(\rho(g)(v)) = \tau(g)(T(v)) = \tau(g)(0) = 0.$$

It follows that $\mathrm{Ker}(T)$ is a subrepresentation of V.

Let $w \in \mathrm{Im}(T)$ and choose $v \in V$ such that $T(v) = w$. Then:

$$\tau(g)(w) = \tau(g)(T(v)) = T(\rho(g)(v)) \in \mathrm{Im}(T).$$

It follows that $\mathrm{Im}(T)$ is a subrepresentation of W. □

Lemma 4.2.2 (Schur)**.** *Let $(\rho, V), (\tau, W)$ be two irreducible representations of G. Then*

$$\mathrm{Hom}_G(V, W) \cong \begin{cases} \mathbb{C}, & (\rho, V) \cong (\tau, W); \\ 0, & \textit{else.} \end{cases} \tag{6}$$

Proof. Let $T \in \mathrm{Hom}_G(V, W)$ and suppose $T \neq 0$. Then $\mathrm{Ker}(T) \neq V$. However, $\mathrm{Ker}(T)$ is a subrepresentation of V and V is irreducible. It follows that $\mathrm{Ker}(T) = 0$ and so that T is injective. Since V is not zero (by definition), $\mathrm{Im}(T) \neq 0$ and since W is irreducible, and $\mathrm{Im}(T)$ is a subrepresentation, $\mathrm{Im}(T) = W$. Thus, T is surjective. It follows that T is an isomorphism. Therefore, if $\mathrm{Hom}_G(V, W) \neq 0$ (and V, W are irreducible) we have $(\rho, V) \cong (\tau, W)$.

It remains to show that if $(\rho, V) \cong (\tau, W)$ then $\mathrm{Hom}_G(V, W)$ is a 1-dimensional vector space. Choose, any non-zero $T \in \mathrm{Hom}_G(V, W)$. We saw that T is then an isomorphism. We get an isomorphism

$$\mathrm{Hom}_G(V, W) \cong \mathrm{End}_G(V), \quad S \mapsto T^{-1} \circ S,$$

and thus it is enough to prove that

$$\mathrm{End}_G(V) \cong \mathbb{C}.$$

Let then $R \in \mathrm{End}_G(V)$ and let λ be an eigenvalue of R. As $\lambda \cdot \mathrm{Id} \in \mathrm{End}_G(V)$, it follows that $R - \lambda \cdot \mathrm{Id} \in \mathrm{End}_G(V)$ and it follows that $\mathrm{Ker}(R - \lambda \cdot \mathrm{Id})$ is a subrepresentation of V. Since every eigenvalue has at least one non-zero eigenvector, we have that $\mathrm{Ker}(R - \lambda \cdot \mathrm{Id}) \neq 0$ and, as V is irreducible, we must have

$$\mathrm{Ker}(R - \lambda \cdot \mathrm{Id}) = V.$$

This means that $R = \lambda \cdot \mathrm{Id}$. This provides the isomorphism $\mathrm{End}_G(V) \cong \mathbb{C}$. □

Remark 4.2.3. Note that the final isomorphism $\mathrm{End}_G(V) \cong \mathbb{C}$ can be given by

$$R \mapsto \frac{1}{\dim(V)} \cdot \mathrm{Tr}(R). \tag{7}$$

4.3. **The space of class functions.** Let G be a finite group and denote by $h(G)$ the class number of G. It appeared before in §**??**. By definition, $h(G)$ is the number of conjugacy classes in G.

Example 4.3.1.

- If G is abelian, $h(G) = \sharp G$.
- If $G = S_n$, $h(G) = p(n)$ (the partition function of n).

A function $f\colon G \to \mathbb{C}$ is called a **class function** if

$$f(hgh^{-1}) = f(g), \quad \forall g, h \in G.$$

Namely, if f is constant on each conjugacy class. We let $\mathrm{Class}(G)$ denote the space of class functions. It is a complex vector space of dimension $h(G)$. If $\phi \in \mathrm{Class}(G)$, define a function $\bar{\phi} \in \mathrm{Class}(G)$ by

$$\bar{\phi}(g) := \overline{\phi(g)}$$

(where on the right we are simply taking the complex conjugate of $\phi(g)$).

We make $\mathrm{Class}(G)$ into a hermitian space by defining an inner product on it:

$$\langle \phi, \psi \rangle := \frac{1}{\sharp G} \sum_{g \in G} \phi(g) \cdot \bar{\psi}(g).$$

It is easy to verify that this is an inner product; we leave that as an exercise. We also define $\|\phi\|$ to be the non-negative real number satisfying $\|\phi\|^2 := \langle \phi, \phi \rangle$. Our main motivation is the following key example.

Example 4.3.2. For any representation (ρ, V) of G, its character $\chi_\rho \in \mathrm{Class}(G)$.

Example 4.3.3. Let $1 \le r \le n$ be integers. Define $\phi_r\colon S_n \to \mathbb{C}$ by $\phi(\sigma)$ equal to the number of cycles of length r appearing in the decomposition of σ as a product of disjoint cycles. The function ϕ_r is a class function.

4.4. **Orthogonality of characters.** We now come to the theorem making characters into a highly powerful tool in the study of representations.

Theorem 4.4.1 (Orthogonality of characters)**.** *Let $(\rho, V), (\tau, W)$ be two irreducible representations of G. Then:*

(1) $\rho \ncong \tau$ then $\langle \chi_\rho, \chi_\tau \rangle = 0$.
(2) $\|\chi_\rho\| = 1$.

Otherwise said, the characters of the irreducible representations of a group G form an orthonormal set in the space of class functions Class(G).

Remark 4.4.2. We will prove in Theorem 7.1.1 below that, in fact, the characters of irreducible representations form an orthonormal *basis* for Class(G).

Proof. Let us write $U = \mathrm{Hom}(V, W)$. We have seen that (σ, U) is a representation of G, where

$$\sigma\colon G \to \mathrm{GL}(U), \quad \sigma(g)(T) = \tau(g) \circ T \circ \rho(g^{-1}),$$

and, by Theorem 4.1.5,

$$\chi_\sigma = \chi_\tau \cdot \bar{\chi}_\rho.$$

By Schur's Lemma,

$$\dim(U^G) = \dim(\mathrm{Hom}_G(V, W)) = \begin{cases} 1, & \rho \cong \tau; \\ 0, & \rho \ncong \tau. \end{cases}$$

On the other hand, by the Projection Formula (Corollary 3.3.2), we have

$$\dim(U^G) = \frac{1}{\sharp G} \sum_{g \in G} \chi_\sigma(g) = \frac{1}{\sharp G} \sum_{g \in G} \chi_\tau(g) \cdot \bar{\chi}_\rho(g) = \langle \chi_\rho, \chi_\tau \rangle.$$

The theorem follows. □

Corollary 4.4.3. *Let h be the number of irreducible characters of G, up to isomorphism. We have*

$$h \leq h(G).$$

In words, the number of irreducible representations of G is at most its class number. (We will see later that $h = h(G)$.)

The following notation will be used repeatedly. Let

$$\rho_1, \dots, \rho_h,$$

be representatives to the isomorphism classes of irreducible representations of G. More precisely, we should say, let $\{(\rho_i, V_i) : i = 1, \dots, h\}$ be representatives to the isomorphism classes of irreducible representations of G, but this is heavier notation that we will usually avoid. In the same vain, given a representation (ρ, V) instead of saying that

$$(\rho, V) \cong (\rho_1, V_1)^{\oplus a_1} \oplus \dots \oplus (\rho_h, V_h)^{\oplus a_h},$$

we will simply write

$$\rho \cong \rho_1^{a_1} \oplus \dots \oplus \rho_h^{a_h}.$$

(Here the a_i are non-negative integers and the notation $(\rho_1, V_1)^{\oplus a_1}$ means the direct sum of (ρ_1, V_1) with itself a_1 times, which is declared to be 0 if $a_1 = 0$.) We will also use the notation

$$d_i = \dim(\rho_i), \quad \chi_i = \chi_{\rho_i}.$$

Finally, whenever we view ρ_i as homomorphisms

$$\rho_i \colon G \to \mathrm{GL}_{d_i}(\mathbb{C}),$$

we will assume that $\{\rho_i(g) : g \in G\}$ are *unitary* matrices, which can always be arranged, as we have seen while proving Maschke's theorem.

4.5. **Unique decomposition.**

We now prove that the decomposition provided by Maschke's theorem is unique.

Theorem 4.5.1. *Let ρ be a representation of G. Then there are unique non-negative integers m_i such that*

$$\rho \cong \rho_1^{m_1} \oplus \dots \oplus \rho_h^{m_h}.$$

Proof. By Maschke's theorem, such m_i always exist. Then, by using the formula for the character of a direct sum (§2.3), we have

$$\chi_\rho = \sum_{i=1}^h m_i \cdot \chi_i.$$

On the other hand, we can use this formula to deduce by orthogonality of characters that

$$\langle \chi_\rho, \chi_j \rangle = \langle \sum_{i=1}^h m_i \cdot \chi_i, \chi_j \rangle = m_j.$$

That shows that the multiplicities m_i are determined uniquely by ρ. □

We will refer to the m_i as the **multiplicity** of the irreducible representation ρ_i in ρ.

Corollary 4.5.2. *We have an isomorphism* $(\rho, V) \cong (\tau, W)$ *if and only if* $\chi_\rho = \chi_\tau$. *In words, the isomorphism class of a representation is completely determined by its character.*

Proof. One of the first properties of characters we proved was that the character depends only on the isomorphism class. So, the "only if" is clear. Suppose now that $\chi_\rho = \chi_\tau$, then for every χ_j we have $\langle \chi_\rho, \chi_j \rangle = \langle \chi_\tau, \chi_j \rangle =: m_j$. We have seen that then both representations are isomorphic to $\rho_1^{m_1} \oplus \cdots \oplus \rho_h^{m_h}$, hence to each other. □

5. Some further theorems and examples

Before proving some additional "big theorems", we study some examples and prove some easier results that will give us a better sense of the whole subject.

5.1. Decomposition of the regular representation.

Recall from § 2.2 the regular representation ρ^{reg} of a group G. It is the representation on the vector space $\mathbb{C}[G]$ that has basis $\{e_g : g \in G\}$, and

$$\rho^{reg}(h)(e_g) = e_{hg}, \quad \forall g, h \in G.$$

We have calculated there that

$$\chi^{reg}(g) = \begin{cases} \sharp G, & g = 1_G; \\ 0, & \text{else.} \end{cases}$$

Let us now find the decomposition of the regular representation into irreducible representations. As we have seen, the multiplicity m_i of χ_i is given by

$$m_i = \langle \chi^{reg}, \chi_i \rangle.$$

This is easy to calculate:

$$\langle \chi^{reg}, \chi_i \rangle = \frac{1}{\sharp G} \sum_g \chi^{reg}(g) \cdot \bar{\chi}_i(g) = \frac{1}{\sharp G} \chi^{reg}(1_g) \cdot \bar{\chi}_i(1_g) = d_i,$$

where $d_i = \dim(V_i)$, as per our conventions. We conclude the following proposition.

Proposition 5.1.1. *We have*

$$\rho^{reg} = \oplus_{i=1}^h \rho_i^{d_i}, \quad \chi^{reg} = \sum_{i=1}^h d_i \chi_i. \tag{8}$$

Namely, every irreducible representation appears in the regular representation with multiplicity equal to its dimension.

By calculating the dimensions of both sides in the isomorphism (8), we conclude:

Corollary 5.1.2. *We have*

$$\sharp G = \sum_{i=1}^h d_i^2. \tag{9}$$

5.2. **Criterion for being irreducible.** An easy consequence of orthogonality of characters is the following useful result.

Corollary 5.2.1. *A representation (ρ, V) is irreducible if and only if*

$$\|\chi_\rho\| = 1.$$

Proof. Let us write

$$\chi_\rho = \sum_i m_i \cdot \chi_i,$$

for non-negative integers m_i. By orthogonality of characters (Pythagoras), we have

$$\|\chi_\rho\|^2 = \sum_i m_i^2.$$

Thus, $\|\chi_\rho\| = 1$ if and only if there exists a unique i_0 such that $i_0 = 1$ and all the rest of 0. But this is exactly the cases where ρ is irreducible. □

Remark 5.2.2. A very similar argument gives that $\|\chi_\rho\|^2 = 2$ if and only if ρ is a sum of two distinct irreducible representations, and that $\|\chi_\rho\|^2 = 3$ if and only if ρ is a sum of three distinct irreducible representations. However, when $\|\chi_\rho\|^2 = 4$ the pattern breaks down, and ρ could be either the sum of four distinct irreducible representations, or isomorphic to two copies of a single irreducible representation.

5.3. **Another look at the standard representation of S^n.** We take another look here at the standard representation of S_n, $n \geq 2$, introduced in Example 3.1.2. Recall that this is an n-dimensional representation ρ^{std} of S_n whose character χ^{std} satisfies

$$\chi^{std}(\sigma) = I(\sigma) = \sharp \text{ fixed points of } \sigma.$$

It is clear that the space of invariant vectors is $(\mathbb{C}^n)^{S_n} = U_1$ in the notation of that example and, in particular, $\dim((\mathbb{C}^n)^{S_n}) = 1$. The projection formula gives another way to calculate this dimension and we get

$$\frac{1}{n!}\sum_{\sigma \in S_n} \chi^{std}(\sigma) = \frac{1}{n!}\sum_{\sigma \in S_n} I(\sigma) = 1.$$

(Note that the latter formula can also be deduced by apply CFF.) This has the pleasant interpretation that *the expected number of fixed points for a randomly chosen permutation is* 1.

Let us use the notation $T = \{1, 2, \dots, n\}$. Then we can say that

$$\|\chi^{std}\|^2 = \frac{1}{n!}\sum_{\sigma \in S_n} (\sharp \text{ fixed points of } \sigma \text{ on } T)^2.$$

Lemma 5.3.1. $\|\chi^{std}\|^2 = 2$.

Proof. Consider the action of S_n on $T \times T$ given by

$$\sigma(i, j) = (\sigma(i), \sigma(j)).$$

It is clear that S_n has two orbits on $T \times T$. Namely, $\{(i, i) : i \in T\}$ and $\{(i, j) : i \neq j \in T\}$. On the other hand, σ fixes (i, j) if and only if $\sigma(i) = i$ and $\sigma(j) = j$. Thus,

$$\sharp \text{ fixed points of } \sigma \text{ on } T \times T = (\sharp \text{ fixed points of } \sigma \text{ on } T)^2.$$

We apply the CFF to the action of S_n on $T \times T$ to conclude that

$$2 = \frac{1}{n!}\sum_\sigma \sharp \text{ fixed points of } \sigma \text{ on } T \times T = \frac{1}{n!}\sum_\sigma (\sharp \text{ fixed points of } \sigma \text{ on } T)^2 = \|\chi^{std}\|^2.$$

□

As we have seen, this implies that ρ^{std} is a sum of two distinct irreducible representations (Remark 5.2.2). But, we also know that

$$\rho^{std} = \mathbb{1} \oplus \rho^{std,0}.$$

Therefore, we conclude that $\rho^{std,0}$ is irreducible. This argument is a much more elegant, I think, than the proof we previously gave.

5.4. **The character group G^* and twisting.** Recall from §2.1 the set

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times),$$

which is group under

$$(\phi_1 \cdot \phi_2)(g) = \phi_1(g) \cdot \phi_2(g).$$

For a 1-dimensional representation there is no difference between the representation and its character. The following properties are not hard to prove and the details are left as an exercise:

(1) We have a canonical isomorphism

$$(G_1 \times \cdots \times G_a)^* = G_1^* \times \cdots \times G_a^*.$$

It is given by

$$f \mapsto (f|_{G_1}, \ldots, f|_{G_a}),$$

where we identify G_i with $\{1\} \times \cdots \times G_i \times \cdots \times \{1\}$. The inverse isomorphism is given by

$$(f_1, \ldots, f_a) \mapsto f_1 \times \cdots \times f_a,$$

where

$$(f_1 \times \cdots \times f_a)(g_1, \ldots, g_a) = f_1(g_1) f_2(g_2) \cdots f_a(g_a).$$

(2) We have a canonical isomorphism $G^* \cong (G^{ab})^*$.

(3) We have a canonical isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\star \cong \mu_n,$$

where $\mu_n = \{e^{j \cdot 2\pi i/n} : j = 0, 1, \ldots, n-1\}$ is the multiplicative group of n-th roots of unity in $\mathbb{C}$. (Don't confuse $(\mathbb{Z}/n\mathbb{Z})^\star$ with $(\mathbb{Z}/n\mathbb{Z})^\times$.) The isomorphism is given by

$$f \mapsto f(1) \in \mu_n,$$

and

$$\zeta \mapsto f \in (\mathbb{Z}/n\mathbb{Z})^\star, \qquad f(a) := \zeta^a.$$

As every finite abelian group is isomorphic to a product of groups of the form $\mathbb{Z}/n\mathbb{Z}$, we have a method to determine G^* for any finite group G:

- Calculate G^{ab}. Any $f\colon G^{ab} \to \mathbb{C}^\times$ induces an element of G^*, i.e., $f \circ \pi$, where $\pi\colon G \to G^{ab}$ is the canonical homomorphism. All multiplicative characters of G arise this way.
- Write $G^{ab} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z}$. Use that $(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z})^* \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_a\mathbb{Z})^*$.
- Use the identification $(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n$.

In particular, we conclude that if G is a finite abelian group then

$$\sharp G = \sharp G^* = h(G).$$

Even better, we can conclude the following corollary of unique decomposition. (For another proof, see the exercises).

Corollary 5.4.1. *Every irreducible representation of an abelian group G is 1-dimensional and there are $\sharp G$ of them. Every n-dimensional representation of G is isomorphic to a representation of the form*

$$\rho\colon G \to \mathrm{GL}_n(\mathbb{C}), \qquad g \mapsto \begin{pmatrix} \alpha_1(g) & & \\ & \ddots & \\ & & \alpha_n(g) \end{pmatrix},$$

for some $\alpha_i \in G^*$.

5.5. **Twisting.** Let (ρ, V) be a representation of G and let $\alpha\colon G \to \mathbb{C}^\times$ be a 1-dimensional representation of G. Then $\mathrm{Hom}((\alpha, \mathbb{C}), (\rho, V))$ is a representation of G of the same dimension and its character, by Theorem 4.1.5, is just

$$\chi_\rho \cdot \bar{\alpha}.$$

As $\bar{\alpha}\colon G \to \mathbb{C}^\times$ is likewise a 1-dimensional representation, we conclude that also $\chi_\rho \cdot \alpha$ is a character. We call the operation $\chi_\rho \mapsto \chi_\rho \cdot \alpha$ **twisting** the representation ρ by the character α. We proved the first part of the following proposition.

Proposition 5.5.1. *For any character χ of G and any 1-dimensional character α of G, also $\chi \cdot \alpha$ is a character. Moreover, if χ is irreducible, so is $\chi \cdot \alpha$.*

Proof. It is not hard to give a direct simple proof of the second part, but let us use characters instead. We have

$$\|\chi\alpha\|^2 = \frac{1}{\sharp G} \sum_g \chi(g)\alpha(g)\bar{\alpha}(g)\bar{\chi}(g).$$

However, because α is 1-dimensional, $\alpha(g)$ is a root of unity and we find

$$\|\chi\alpha\|^2 = \frac{1}{\sharp G} \sum_g \chi(g)\bar{\chi}(g) = \|\chi\|^2 = 1.$$

Thus, by Corollary 5.2.1, χ is irreducible. □

Remark 5.5.2. It is possible that $\chi \cdot \alpha = \chi$ even if $\alpha \neq \mathbb{1}$. In fact, this happens quite often, for example in cases that G has a unique irreducible representation of a given dimension. Nevertheless, in general, twisting by 1-dimensional characters is a very useful method to get new irreducible representations from known ones.

6. Character tables

The character table of a group G is one of the best ways to get insight into the structure of G and its action on vector spaces. There are whole books written on this subject.[2] In this section we will study various properties of the character table. Our treatment is by no means exhaustive, or complete (we will mention a few properties that we will not prove).

The characters table of G has rows for every irreducible representation of G, and columns for every conjugacy class of G. We reserve the first row for the character $\mathbb{1}$ and the first column for the conjugacy class of the identity (often we will write a representative element for each conjugacy class, and indicate below the conjugacy class how many elements it contains). The table entry corresponding to a character χ and a conjugacy class c is just $\chi(c)$. By that we mean $\chi(x)$ for any $x \in c$; the choice of x doesn't influence the value $\chi(x)$. So, for example, the character table of S_3 is the following:

	1	(12)	(123)
	1	3	2
$\chi_1 = \mathbb{1}$	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

TABLE 1. Character table of S_3

We see the three representatives $1, (12), (123)$ to the distinct conjugacy classes of S_3 and their sizes indicated by $1, 3, 2$. We see 3 irreducible characters. The first one is the trivial character $\mathbb{1}$, the second is the sign homomorphism $\mathrm{sgn}\colon S_3 \to \mathbb{C}^\times$, and the third is the character $\chi^{std,0}$.

We will usually use the notation χ_i for the rows and c_i for the columns. We use the notation introduced before: χ_i is the character of the irreducible representation ρ_i that has dimension d_i.

6.1. First properties of the character table.

Theorem 6.1.1. *The character table of G has the following properties:*

(1) The number of rows equals to the number of columns.
(2) The sum of the squares of the entries of the first column is the cardinality of the group.
(3) The number of rows with 1 *in the first column is equal to* $\sharp G^{ab}$.
(4) Every entry in the first column is an integer dividing $\sharp G$.
(5) The "weighted" inner-product of distinct rows is 0. *The weighted self-product of a row is equal to* $\sharp G$ *(here the weights are the cardinality of conjugacy classes).*
(6) The "weighted" sum of the rows is the vector $(\sharp G, 0, \ldots, 0)$ *(here the weights are the dimensions of the representations).*

The proof consists of references to theorems we proved, or will prove shortly.

Proof. (1) is the statement that the number of irreducible characters h is actually equal to $h(G)$. We mentioned this before and will prove it in Theorem 7.1.1 below.

(2) is Corollary 5.1.2: $\sharp G = \sum_{i=1}^h d_i^2$

(3) states the the irreducible characters of dimension 1 are 1-dimensional characters $g \to \mathbb{C}^\times$, and $\sharp G^* = \sharp (G^{ab})^*$ (Lemma 2.1.1).

(4) is a theorem we will not prove because it requires some notions from algebraic number theory, but it is useful to know.

(5) is just orthogonality of characters (Theorem 4.4.1). If we use the fact that characters are class functions, we may write

$$\langle \chi_i, \chi_j \rangle = \frac{1}{\sharp G} \sum_{g \in G} \chi_i(g) \bar{\chi}_j(g) = \frac{1}{\sharp G} \sum_{i=1}^{h} |c_i| \cdot \chi_i(c_i) \bar{\chi}_j(c_i).$$

We find that if $i \neq j$ then the weighted inner-product of the rows, $\sum_{i=1}^h |c_i| \chi_i(c_i) \bar{\chi}_j(c_i)$, is equal to 0, and if $i = j$ it is equal to $\sharp G$.

(6) is just a restatement of the decomposition of the regular representation: $\chi^{reg} = \sum_{i=1}^h d_i \chi_i$ (Proposition 5.1.1). □

[2] For example: I. Martin Isaacs, *"Character Theory of Finite Groups"*, Dover 1994.

6.2. **Examples of character tables.**

6.2.1. *The character table of $\mathbb{Z}/n\mathbb{Z}$.* Recall that every irreducible representation of an abelian group is a multiplicative character and that we have

$$(\mathbb{Z}/n\mathbb{Z})^* \cong \mu_n.$$

We usually denote the corresponding characters $\rho_0, \dots, \rho_{n-1}$ in this case, because if we let $\zeta = e^{2\pi i/n}$ then we have

$$\rho_i(a) = \zeta^{ai}.$$

(This notation is slightly in odds with the usual convention of denoting the irreducible characters of a group G by $\chi_1, \dots, \chi_h$.) We find the following table

	0	1	2		$n-1$
$\rho_0 = \mathbb{1}$	1	1	1	$\dots$	1
ρ_1	1	ζ	ζ^2	$\dots$	ζ^{n-1}
ρ_2	1	ζ^2	ζ^4	$\dots$	$\zeta^{2(n-1)}$
$\vdots$				$\vdots$	
ρ_{n-1}	1	ζ^{n-1}	$\zeta^{2(n-1)}$	$\dots$	$\zeta^{(n-1)^2}$

TABLE 2. Character table of $\mathbb{Z}/n\mathbb{Z}$

Note that property (6) in Theorem 6.1.1 gives us the very useful fact in complex analysis: For a root of unity ζ of order n, we have $\sum_{i=0}^{n-1} \zeta^{ai} = 0$ for every $a \not\equiv 0(n)$.

6.2.2. *The character tables of $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z})^2$.* Multiplying two copies of the character table of $\mathbb{Z}/2\mathbb{Z}$ we find

	0	1
$\mathbb{1}$	1	1
ρ_1	1	-1

$\times$

	0	1
$\mathbb{1}$	1	1
ρ_1	1	-1

$=$

	(0,0)	(1,0)	(0, 1)	(1,1)
$\mathbb{1} \times \mathbb{1}$	1	1	1	1
$\mathbb{1} \times \rho_1$	1	1	-1	-1
$\rho_1 \times \mathbb{1}$	1	-1	1	-1
$\rho_1 \times \rho_1$	1	-1	-1	1

TABLE 3. Character table of $(\mathbb{Z}/2\mathbb{Z})^2$

Similarly, for any abelian group $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z}$ we can multiply the character tables for each $\mathbb{Z}/n_i\mathbb{Z}$ to find the character table of G. This rests on our results

$$G^* \cong (\mathbb{Z}/n_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/n_a\mathbb{Z})^* \cong \mu_{n_1} \times \cdots \times \mu_{n_a},$$

and the concrete description of the character table of $\mathbb{Z}/n\mathbb{Z}$.

It is not efficient to use this method for $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ because by CRT we have $G \cong \mathbb{Z}/15\mathbb{Z}$ which is a cyclic group for which we already have a nice description. But, for example, for the case $G = (\mathbb{Z}/3\mathbb{Z})^2$ it is useful, and we find the following 9×9 table ($\omega = e^{2pii/3}$):

	0	1	2
$\mathbb{1}$	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$\times$

	0	1	2
$\mathbb{1}$	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$=$

	(0,0)	...	(1, 2)	...	(a, b)
$\mathbb{1} \times \mathbb{1}$	1		1		1
$\vdots$					
$\rho_1 \times \rho_2$	1		ω^2		ω^{a+2b}
$\vdots$		$\vdots$		$\vdots$	
$\rho_i \times \rho_j$	1		ω^{i+2j}		ω^{ai+bj}
$\vdots$		$\vdots$		$\vdots$	

TABLE 4. Character table of $(\mathbb{Z}/3\mathbb{Z})^2$

6.2.3. *The character table of* S_3. We have $h(S_3) = p(3) = 3$ and so there are 3 conjugacy classes and we take as representatives $1, (12), (123)$. Their sizes are $1, 3, 2$, respectively. We have

$$S_3^{ab} = S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z},$$

and, in fact, we know two 1-dimensional characters: $\mathbb{1}$ and sgn. As we must have

$$\sharp S_3 = 6 = 1^1 + 1^1 + x^2,$$

we conclude that the remaining irreducible representation of S_3 is 2-dimensional. We happen to know such a representation, namely, $\rho^{std,0}$ and its character $\chi^{std,0}$ whose value on a permutation σ is the number of fixed points of σ minus 1. We therefore find the following table:

	1	(12)	(123)
	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

TABLE 5. Character table of S_3

Remark though that we didn't really need to use our "lucky break" of knowing before-hand an irreducible 2-dimensional representation. We could have solved for the remaining character:

$$\chi_3 = \frac{1}{2}(\chi^{reg} - \chi_1 - \chi_2)$$

(Theorem 6.1.1).

6.2.4. *The character table of* D_4. It requires some calculations but one find that

$$D_4' = \{1, x^2\}, \quad D_4^{ab} = \{1, \bar{x}, \bar{y}, \bar{x}y\},$$

and that every element of D_4^{ab} has order 2. Thus,

$$D_4^{ab} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad x \mapsto (1, 0), y \mapsto (0, 1).$$

We also calculate "by hand" the conjugacy classes and find that they are given by

$$c_1 = \{1\},\ c_2 = \{x, x^{-1}\},\ c_3 = \{x^2\},\ c_4 = \{y, yx^2\},\ c_5 = \{yx, yx^{-1}\}.$$

There isn't a really quick way to do that, but one can note that since $\langle x \rangle$ is a normal subgroup, conjugacy classes are either contained in it, or disjoint from it. At any rate, we now know that D_4 has four 1-dimensional representations, "lifted" from $(\mathbb{Z}/2\mathbb{Z})^2$. That is, if χ is an irreducible character of $(\mathbb{Z}/2\mathbb{Z})^2$ and f is the composition $D_4 \to D_4^{ab} \to (\mathbb{Z}/2\mathbb{Z})^2$ then $\chi \circ f$ is an 1-dimensional character of D_4. In addition, D_4 has one more irreducible representation and its dimension x satisfies

$$8 = \sharp D_4 = 1^2 + 1^2 + 1^2 + 1^2 + x^2.$$

It follows that we are missing a 2-dimensional representation. Note that we can solve for the missing character, say χ, using the result on the sum of the rows of the character table, but it is also natural to wander whether the missing representation is provided by the action of D_4 on the plane (the action inducing the action of D_4 on the square). In this representation ρ^{pl}, the action of the representatives for conjugacy classes is given as follows:

$$1 = \left(\begin{smallmatrix} 1 & \\ & 1 \end{smallmatrix}\right), \ x = \left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right), \ y = \left(\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right), \ x^2 = \left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right), \ yx = \left(\begin{smallmatrix} & -1 \\ -1 & \end{smallmatrix}\right).$$

We can now write the character table of D_4. The last row is $\chi^{pl} = \chi_{\rho^{pl}}$, which is indeed irreducible because $\|\chi^{pl}\| = 1$.

	1	x	y	xy	x^2
	1	2	2	2	1
$\mathbb{1}$	1	1	1	1	1
$\rho_1 \times \mathbb{1}$	1	-1	1	-1	1
$\mathbb{1} \times \rho_1$	1	1	-1	-1	1
$\rho_1 \times \rho_1$	1	-1	-1	1	1
χ^{pl}	2	0	0	0	-2

TABLE 6. Character table of D_4

Here is an application. The composition ρ defined by

$$\begin{tikzcd} D_4 \arrow[r] & S_4 \arrow[r, "\rho^{std}"] & \mathrm{GL}_4(\mathbb{C}) \end{tikzcd},$$

(where the first arrow is the natural inclusion of D_4 into S_4, $x \mapsto (1234), y \mapsto (24)$) is a 4-dimensional representation of D_4. It is a bit hard to understand this action. In terms of matrices

$$x = \begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix}, \quad y = \begin{pmatrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \end{pmatrix}.$$

However, we can decompose ρ into irreducible representations. A calculation gives

$$\langle \chi_\rho, \mathbb{1} \rangle = 1 \quad , \langle \chi_\rho, \rho_1 \times \mathbb{1} \rangle = 1, \quad \langle \chi_\rho, \chi^{pl} \rangle = 1.$$

This tells us that

$$\rho \cong \mathbb{1} \oplus (\rho_1 \times \mathbb{1}) \oplus \rho^{plane}.$$

That means that there is another basis for $\mathbb{C}^4$ in which the representation has the form

$$x = \begin{pmatrix} 1&0&0&0 \\ 0&-1&0&0 \\ 0&0&0&1 \\ 0&0&-1&0 \end{pmatrix}, \quad y = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&-1&0 \\ 0&0&0&1 \end{pmatrix}.$$

And a general element g of D_4 will act by a matrix of the form

$$\begin{pmatrix} 1&0&0 \\ 0&\pm1&0 \\ 0&0&\rho^{pl}(g) \end{pmatrix}.$$

It is much easier now to understand the action of D_4.

6.2.5. *The character table of S_4.*

Here is a general principle. Let $f\colon A \to B$ be a homomorphism of groups. Let $\rho\colon B \to \mathrm{GL}(V)$ be a representation of B. Then $\rho \circ f$ is a representation of A and its character is simply

$$\chi_{\rho\circ f} = \chi_\rho \circ f\colon A \to \mathbb{C}.$$

In fact, we have used it several times before in the situation $G \to G^{ab} \to \mathbb{C}^\times$ to lift 1-dimensional characters of G^{ab} to G.

Now, if f is *surjective* and ρ is irreducible then also $\rho \circ f$ is irreducible. Indeed, suppose that $U \subseteq V$ is a subrepresentation of $\rho \circ f$. That is, for all $a \in A$ we have $\rho(f(a))(U) \subseteq U$. Then, as f is surjective, it follows that for all $b \in B$ we have $\rho(b)(U) \subseteq U$. It follows that U is a subrepresentation of ρ and so $U = 0$ or V.

Let us use this for the surjective homomorphism $f\colon S_4 \to S_3$, whose kernel is K, the Kline group. We have studied this homomorphism before. Using it, we can lift the characters of S_3 to S_4, and so we easily find the first 3 rows of the character table of S_4. (The conjugacy classes of S_n correspond to the cycle type of permutations and that gives us the columns' labels.) As there are 5 conjugacy classes, there are two additional irreducible representations. We know one of them, $\rho^{std,0}$, and we get the last row as either the twist $\rho^{std,0} \cdot \mathrm{sgn}$, or by solving the equation where the sum of the rows with multiplicities is equal to the vector $(24, 0, 0, 0, 0)$. At any rate, we find the following.

	1	(12)	(123)	(1234)	(12)(34)
	1	6	8	6	3
$\mathbb{1}$	1	1	1	1	1
sgn	1	-1	1	-1	1
$\chi_3 \circ f$	2	0	-1	0	2
$\chi^{std,0}$	3	1	0	-1	-1
$\chi^{std,0} \cdot \mathrm{sgn}$	3	-1	0	1	-1

TABLE 7. Character table of S_4

6.2.6. *Character table of A_4.* The representatives for the conjugacy classes are $1, (12)(34), (123), (132)$. There are therefore 4 irreducible representations. As A_4/K is of order 3, it follows that $A_4/K \cong \mathbb{Z}/3\mathbb{Z}$ and that $K \supseteq A_4'$. As A_4 is not abelian, $A_4' \neq \{1\}$ and so contains some element of cycle type $(2, 2)$. But those form a single conjugacy class and A_4' is normal. It follows that $A_4' = K$.

We conclude that there are 4 irreducible representations, of which 3 are 1-dimensional, and the last is 3-dimensional (as $\sharp A_4 = 1^2 + 1^2 + 1^2 + x^2$ only allows $x = 3$). Using the result about the sum of rows we find the following character table:

	1	(123)	(132)	(12)(34)
	1	4	4	3
$\mathbb{1}$	1	1	1	1
χ_1	1	ω	ω^2	1
χ_2	1	ω^2	ω	1
χ	3	0	0	-1

TABLE 8. Character table of A_4

It turns out that the last character is just $\chi^{std,0}|_{A_4}$. This is no coincidence. One can prove that for $n \geq 4$ the representation $\rho^{std,0}|_{A_n}$ is an irreducible representation of A_n (Exercise **??**).

6.3. **Orthogonality of columns.** In this subsection we show that the columns of the character table enjoy an orthogonality property. We begin with some renormalization device to make the argument more transparent, hopefully.

For every character χ of G (or even for every class function f), we define a vector $v_\chi \in \mathbb{C}^h$, where $h = h(G)$ is the number of conjugacy classes of G. Let $c_1, \ldots, c_h$ be the conjugacy classes of G, and let

$$v_\chi = (\sqrt{\frac{\sharp c_1}{\sharp G}} \cdot \chi(c_1), \ldots, \sqrt{\frac{\sharp c_h}{\sharp G}} \cdot \chi(c_h))$$

The point of this construction is that for every two characters χ, ψ (or even any two class functions) we have

$$\langle \chi, \psi \rangle = \langle v_\chi, v_\psi \rangle,$$

where the inner-product on the left is the inner product of class-functions, and the inner-product on the right is the usual inner-product in $\mathbb{C}^h$. In fact, we have already noticed something very similar – see the proof of part (5) of Theorem 6.1.1.

Let $\chi_1, \ldots, \chi_h$ denote the irreducible characters of G. It follows that the rows of the following matrix are orthonormal:

$$\left(\begin{array}{c} v_{\chi_1} \\ \hline v_{\chi_2} \\ \hline \vdots \\ \hline v_{\chi_h} \end{array} \right).$$

But this implies that the columns of the same matrix are an orthonormal set too. Namely, for any two conjugacy classses c_a, c_b we get that

$$\sum_{i=1}^{h} \sqrt{\frac{\sharp c_a}{\sharp G}} \sqrt{\frac{\sharp c_b}{\sharp G}} \cdot \chi_i(c_a) \bar{\chi}_i(c_b) = \delta_{ab}.$$

Note that $\sharp(G)/\sharp(c_a) = \sharp Cent(x)$ for any $x \in C_a$. Therefore, we conclude the following.

Proposition 6.3.1 (Orthogonality of columns)**.** *We have the following orthogonality properties of the columns of the character table.*

(1) If $c_a \neq c_b$ are conjugacy classes then the product of the c_a column with the c_b column is 0*. To be precise:*

$$\sum_{i=1}^{h} \chi_i(c_a) \bar{\chi}_i(c_b) = 0.$$

(2) For every conjugacy class c_a the norm of the c_a column is the cardinality of its centralizer. That is,

$$\sum_{i=1}^{h} |\chi_i(c_a)|^2 = \sharp Cent(x), \quad x \in c_a.$$

It follows that we can use the entries of the character table, more specifically we can use the second part of the proposition, to figure out the size of conjugacy classes. We record it as a corollary.

Corollary 6.3.2. *The character table determines the size of the conjugacy classes.*

7. THE IRREDUCIBLE CHARACTERS FORM A BASIS FOR CLASS(G)

In this section we fill a gap and prove that the irreducible characters of a group G form a basis for Class(G). Nothing prevented us from proving it sooner; it just seemed more useful to see some examples before developing the theory further.

7.1. **Irreducible characters form a basis.**

Theorem 7.1.1. *Let G be a group and let $\chi_1, \dots, \chi_h$ be its irreducible characters. Then*

$$\{\chi_1, \dots, \chi_h\}$$

is an orthonormal basis for Class(G).

Proof. We begin with a lemma that constructs endomorphisms of representations.

Lemma 7.1.2. *Let (ρ, V) be a representation of G and let α a class function. Then the linear operator*

$$T = T_\rho = \sum_{g \in G} \alpha(g)\rho(g) \in \mathrm{End}_G(V).$$

Proof. The fact that T is a linear operator is clear, because $\alpha(g)$ are scalars and T is the sum of the linear operators $\alpha(g)\rho(g)$. The point is that it commutes with ρ. We have

$$\rho(h) \circ T \circ \rho(h)^{-1} = \sum_{g \in G} \alpha(g)\rho(hgh^{-1}) = \sum_{g \in G} \alpha(hgh^{-1})\rho(hgh^{-1}).$$

The last equality is true because α is a class function. Now, $g \mapsto hgh^{-1}$ is a bijection of G (even an automorphism) and hence

$$\rho(h) \circ T \circ \rho(h)^{-1} = \sum_{g \in G} \alpha(hgh^{-1})\rho(hgh^{-1}) = \sum_{g \in G} \alpha(g)\rho(g) = T.$$

□

We know already that $\{\chi_1, \dots, \chi_h\}$ are an orthonormal set. To prove they form a basis we need only show for $\beta \in \mathrm{Class}(G)$,

$$\langle \chi_i, \beta \rangle = 0, \forall i \implies \beta \equiv 0.$$

Let $\alpha = \bar{\beta}$. It will of course be enough to prove $\alpha \equiv 0$.

Let (ρ, V) be an irreducible representation. We claim the the operator

$$T_\rho := \sum_{g \in G} \alpha(g)\rho(g) \in \mathrm{End}_G((\rho, V))$$

is actually the zero operator. By Schur's Lemma, we have $\mathrm{End}_G((\rho, V)) \cong \mathbb{C}$ under the map $T \mapsto \frac{1}{\dim(V)}\mathrm{Tr}(T)$ (Equation (7)). If we apply to T_ρ we find that

$$\frac{1}{\dim(V)}\mathrm{Tr}(T_\rho) = \sum_{g \in G} \alpha(g)\mathrm{Tr}(\rho(g)) = \sum_{g \in G} \chi_\rho(g)\bar{\beta}(g) = \sharp G \langle \chi_\rho, \beta \rangle = 0.$$

And therefore $T_\rho = 0$.

Note that the construction

$$\rho \mapsto T_\rho = \sum_{g \in G} \alpha(g)\rho(g)$$

commutes with direct sums. Thus, we may conclude that for *any* representation (ρ, V) of G we have $T_\rho = 0$. In particular this holds of the regular representation. That is, we conclude that $\sum_{g\in G} \alpha(g)\rho^{reg}(g)$ is the zero operator on $\mathbb{C}[G]$. In this case, we must have

$$\sum_{g\in G} \alpha(g)\rho^{reg}(g)(e_1) = 0,$$

where $e_1 \in \{e_g : g \in G\}$ is the basis vector indexed by the identity element of G. However,

$$\sum_{g\in G} \alpha(g)\rho^{reg}(g)(e_1) = \sum_{g\in G} \alpha(g)e_g.$$

As $\{e_g\}$ is a basis, it follows that $\alpha(g) = 0$ for all $g \in G$, as we wanted to show. □

7.2. **Even more properties of the character table.** We organize together all the properties of the character table we have seen, implicitly or explicitly.

Theorem 7.2.1. *Let G be a group with class number h. Let $\{\chi_i : i = 1, \dots, h\}$ be its irreducible characters, $d_i = \dim(\chi_i) = \chi_i(1)$, and let $\{c_a : a = 1, \dots, h\}$ be the conjugacy classes of G. We assume always that $\chi_1 = \mathbb{1}$ and $c_1 = \{1_g\}$.*

The character table of G has the following properties:

(1) The number of rows equals to the number of columns.
(2) The sum of the squares of the entries of the first column is the cardinality of the group.
(3) The number of rows with 1 in the first column is equal to $\sharp G^{ab}$.
(4) Every entry in the first column is an integer dividing $\sharp G$.
(5) The "weighted" inner-product of distinct rows is 0. The weighted self-product of a row is equal to $\sharp G$ (here the weights are the cardinality of conjugacy classes).
(6) The "weighted" sum of the rows is the vector $(\sharp G, 0, \dots, 0)$ (here the weights are the dimensions of the representations).
(7) For any two columns c_a, c_b we have

$$\sum_{i=1}^{h} \chi_i(c_a)\bar{\chi}_i(c_b) = 0, \quad a \neq b,$$

and

$$\sum_{i=1}^{h} |\chi_i(c_a)|^2 = |Cent(x)|, \; x \in c_a.$$

(8) If $\chi_i(c_a) = \alpha$ then $\chi_i(c_a^{-1}) = \bar{\alpha}$ where c_a^{-1} is the conjugacy class $\{x^{-1} : x \in c_a\}$. In particular, the set of entries of the character table is closed under complex conjugation.
(9) If χ_i is 1-dimensional and χ_j is any other irreducible character, then $\chi_i \cdot \chi_j = \chi_k$ for some irreducible character χ_k (possibly equal to χ_j).
(10) $|\chi_i(g)| \leq \chi_i(1)$, with equality if and only if $\rho_i(g) = \alpha \cdot Id$ for some root of unity α.
(11) If $c_a \neq c_b$ then there is some character χ_i such that $\chi_i(c_a) \neq \chi_i(c_b)$.

Proof. We have already proved properties (1) - (6) in Theorem 6.1.1 (only that now we have really proved (1)). Property (7) is the orthogonality of columns proven in Proposition 6.3.1. Property (8) was also mentioned before: we have seen that $\chi_i(x^{-1}) = \overline{\chi_i(x)}$ (Equation 5). Property (9) is of course the twisting operation we have studied in § 5.5. Property (10) follows from the fact that $\chi_i(g)$ is a sum of d_i roots of unity and the absolute value is equal to d_i if and only if they all point in the same direction. The last property follows from the fact that the $\{\chi_i\}$ form a basis for the class functions and so for any given $c_a \neq c_b$ a suitable linear combination of them should have value 1 on c_a and value 0 on c_b. This is only possible if for some i, $\chi_i(c_a) \neq \chi_i(c_b)$. □

Character tables have even more properties. We mention an additional one, which is a theorem of Burnside, just because it is so easy to state. We will not use it in this course: *If $d_i > 1$ then χ_i takes the value 0 for some conjugacy class.*

8. Using the character table to find normal subgroups

We will now see a beautiful application of character tables for the calculation of all normal subgroups of a group G.

8.1. Normal subgroups and character kernels.

Let (ρ, V) be any representation of G with character χ. Define

$$\mathrm{Ker}(\chi) := \{g \in G : \chi_\rho(g) = \chi(1)\} = \{g \in G : \chi_\rho(g) = \dim(V)\}.$$

Lemma 8.1.1. *We have*

$$\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho),$$

and so $\mathrm{Ker}(\chi)$ *is a normal subgroup of G.*

Proof. Let $g \in \mathrm{Ker}(\rho)$ then $\rho(g) = \mathrm{Id}_V$. Then, $\chi(g) = \mathrm{Tr}(\mathrm{Id}_V) = \dim(V)$ and thus $g \in \mathrm{Ker}(\chi)$.

Conversely, let $g \in \mathrm{Ker}(\chi)$ and $d = \dim(V)$. As $\chi(g)$ is a sum of d roots of unity (which are the eigenvalues, with multiplicity, of $\rho(g)$), the only way this sum can be equal to to d if all these roots of unity are 1. This implies $\rho(g) = \mathrm{Id}_V$. □

In particular, if $\chi_1, \dots, \chi_h$ denote the irreducible characters of G, as per our usual notation, we have the normal subgroups

$$\mathrm{Ker}(\chi_i), \quad i = 1, 2, \dots, h.$$

Note that these subgroups can be written as a union of conjugacy classes, given the character table of G.

Lemma 8.1.2. *Let χ be a character of a representation (ρ, V) of G. Suppose that*

$$\chi = \sum_{i \in I} a_i \chi_i,$$

for a subset $I \subseteq \{1, 2, \dots, h\}$ and positive integers a_i. Then,

$$\mathrm{Ker}(\chi) = \cap_{i \in I} \mathrm{Ker}(\chi_i).$$

Once more, note that this can be calculated effectively from the character table of G.

Proof. We have

$$\chi(1) = \sum_{i \in I} a_i \chi_i(1).$$

If $g \in \mathrm{Ker}(\chi_i)$ for every i, then

$$\chi(g) = \sum_{i \in I} a_i \chi_i(g) = \sum_{i \in I} a_i \chi_i(1) = \chi(1),$$

and so $g \in \ker(\chi)$.

Conversely, if $g \in \ker(\chi)$ we have

$$\chi(1) = \chi(g) = \sum_{i \in I} a_i \chi_i(g) = \sum_{i \in I} a_i \chi_i(1).$$

Since the a_i are positive integers and $|\chi_i(g)| \leq \chi_i(1)$, the only way the last equality can hold is if $\chi_i(g) = \chi_i(1)$ for every $i \in I$. Namely, if $g \in \mathrm{Ker}(\chi_i)$, for all $i \in I$. □

Lemma 8.1.3. *Any normal subgroup $N \lhd G$ is of the form* $\mathrm{Ker}(\chi)$ *for some character χ.*

Proof. Let $H = G/N$ and consider the composition

$$G \xrightarrow{\pi} G/N = H \xrightarrow{\rho_H^{reg}} \mathrm{GL}(\mathbb{C}[H]).$$

Let $\rho = \rho_H^{reg} \circ \pi$. Since the regular representation ρ_H^{reg} of H is injective, we have $\mathrm{Ker}(\rho) = \mathrm{Ker}(\pi) = N$. Therefore,

$$N = \mathrm{Ker}(\chi_\rho).$$

□

We summarize our discussion in the following theorem.

Theorem 8.1.4. *Let $\chi_1, \dots, \chi_h$, $h = h(G)$, be the irreducible characters of G. Let*

$$N_i = \mathrm{Ker}(\chi_i).$$

Any normal subgroup N of G is of the form

$$N = \cap_{i \in I} \mathrm{Ker}(\chi_i),$$

for a suitable subset $I \subseteq \{1, 2, \dots, h\}$. And, conversely, any such intersection is a normal subgroup of G.

Remark 8.1.5. The whole point is, of course, that we have a practical easy method to find all the normal subgroups of a group G from the character table. Note, also, that the theorem implies that any proper maximal normal subgroup of G is of the form $\mathrm{Ker}(\chi_i)$ for some i (although, the converse is not true; $\mathrm{Ker}(\chi_i)$ is often not a maximal normal subgroup).

Example 8.1.6. We illustrate the theorem using the character table of A_4. Recall that it is given by the following table, where in the last column we indicated the kernel of the character.

	1	(123)	(132)	(12)(34)	Ker
	1	4	4	3	
$\mathbb{1}$	1	1	1	1	A_4
χ_1	1	ω	ω^2	1	K
χ_2	1	ω^2	ω	1	K
χ	3	0	0	-1	$\{1\}$

TABLE 9. Character table of A_4

We conclude that A_4 has only one non-trivial normal subgroup, which is K.

8.2. **Recognizing the commutator subgroup.** Given a group G we have several normal subgroups canonically associated to it. For example, the commutator subgroup G' and the centre $Z(G)$. In light of Theorem 8.1.4, it makes sense to ask how to construct them from the character table. For the center, this is just the union of all conjugacy classes of size 1. For the commutator subgroup we have the following proposition.

Proposition 8.2.1. *We have*

$$G' = \bigcap_{\chi \text{ 1-dim. char.}} \mathrm{Ker}(\chi).$$

Proof. Suppose that $g \in G'$ and ρ is a 1-dimensional representation, then $\rho(G') = 1$ (and so, as we have used several times before, ρ factors through G^{ab}). Thus, $G' \subseteq \bigcap_{\chi \text{ 1-dim. char.}} \mathrm{Ker}(\chi)$.

Suppose now that $g \notin G'$ and denote $\bar{g}$ its image in G^{ab}. Then $\bar{g} \neq 0$ (the identity element of the abelian group G^{ab}). Write

$$G^{ab} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_a\mathbb{Z}.$$

Then $\bar{g} = (g_1, \dots, g_a)$ and assume without loss of generality that $g_1 \neq 0$.

Let $\zeta = e^{2\pi i/n_1}$ and ρ the multiplicative character of $\mathbb{Z}/n_1\mathbb{Z}$ given by $\rho(a) = \zeta^a$. Then, $\rho \times \mathbb{1} \times \cdots \times \mathbb{1}$ is a multiplicative character of G^{ab} and hence, through $G \to G^{ab}$, also of G. We have

$$(\rho \times \mathbb{1} \times \cdots \times \mathbb{1})(g) = (\rho \times \mathbb{1} \times \cdots \times \mathbb{1})(\bar{g}) = \rho(g_1) = \zeta^{g_1} \neq 1.$$

Thus, $g \notin \bigcap_{\chi \text{ 1-dim. char.}} \mathrm{Ker}(\chi)$, and the proof is complete. □

9. Some more examples of representations

In this section we consider two more examples of representations, more difficult that we considered thus far.

9.1. **The character table of the Frobenius group F_{20}.** The Frobenius group F_{20} is the group

$$\mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^\times.$$

Recall that $(\mathbb{Z}/5\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ and the semi-direct product is taken relative to the identity map $(\mathbb{Z}/5\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$. The group law is very simple,

$$(n_1, b_1)(n_2, b_2) = (n_1 + b_1 n_2, b_1 b_2), \qquad n_i \in N := \mathbb{Z}/5\mathbb{Z}, b_i \in B := (\mathbb{Z}/5\mathbb{Z})^\times.$$

The Frobenius group can be realized into other ways:

(1) As a group of matrices

$$\left\{ \begin{pmatrix} b & n \\ & 1 \end{pmatrix} : b \in \mathbb{Z}/5\mathbb{Z}^\times, n \in \mathbb{Z}/5\mathbb{Z} \right\},$$

with multiplication

$$\begin{pmatrix} b_1 & n_1 \\ & 1 \end{pmatrix} \begin{pmatrix} b_2 & n_2 \\ & 1 \end{pmatrix} = \begin{pmatrix} b_1 b_2 & n_1 + b_1 n_2 \\ & 1 \end{pmatrix}.$$

(2) As the subgroup of S_5 given by

$$\langle (12345), (2354) \rangle.$$

The isomorphism of F_{20} with the group of matrices is evident. For the realization as the subgroup of permutations, we send

$$(12345)^n \mapsto (n, 1), \qquad (2345) \mapsto (0, 2).$$

Because

$$(2354)(12345)(2354)^{-1} = (12345)^2,$$

and $(0,2)(1,1)(0,2)^{-1} = (2,1)$, it follows (with some additional arguments) that we have an isomorphism $\langle (12345), (2354) \rangle \cong F_{20}$.

Next, we calculate the conjugacy classes of F_{20}. For elements of N, conjugation by N is trivial and so by conjugating by elements of B we get the full conjugacy classes (using that $F_{20} = NB$). We have the formula

$$(0, b)(n, 1)(0, b^{-1}) = (bn, 1).$$

We find two conjugacy classes:

$$a_1 = \{(0, 1)\}, \quad a_2 = \{(i, 1) : i = 1, 2, 3, 4\}.$$

Likewise, when we conjugating elements of B by B is trivial and so we will get the full conjugacy classes of elements of B by conjugating them by elements of N. We have the relation

$$(n,1)(0,b)(-n,1) = ((1-b)n, b).$$

For $b = 2,3,4$, we get the conjugacy classes

$$c_2 = \{(i,2) : 0 \le i \le 4\}, \quad c_3 = \{(i,3) : 0 \le i \le 4\}, \quad c_4 = \{(i,4) : 0 \le i \le 4\}.$$

We see that we already accounted for all the elements of the group. Therefore, F_{20} has 5 conjugacy classes (of sizes $1,4,5,5,5$).

Note that $F_{20}/N \cong B \cong (\mathbb{Z}/5\mathbb{Z})^\times$, $(n,b) \mapsto b$. As F_{20} is not abelian, and N has no non-trivial subgroups, it follows that $N = F_{20}'$ and $F_{20}^{ab} \cong (\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic group of order 4 with generator 2.Thus, F_{20} has precisely 5 irreducible representations, 4 of which are 1-dimensional. Therefore, as the size of the group is the sum of the squares of the dimensions of the irreducible representations, the remaining irreducible representation is 4-dimensional. We can find its character χ_4 by using that the weighted sum of the rows of the character table is the regular representation. (The notation is chosen so that the first 4 characters have notation that agrees with the notation we used for cyclic groups.)

	a_1	a_2	c_2	c_3	c_4
	1	4	5	5	5
	(0, 1)	(1, 1)	(0,2)	(0, 3)	(0, 4)
$\chi_0 = \mathbb{1}$	1	1	1	1	1
χ_1	1	1	i	$-i$	-1
χ_2	1	1	-1	-1	1
χ_3	1	1	$-i$	i	-1
χ_4	4	-1	0	0	0

TABLE 10. Character table of F_{20}

It is not hard to check that under the realization of F_{20} as a subgroup of S_5 in fact $\chi_4 = \chi^{std,0}|_{F_{20}}$. Cf. Exercise 9.1.1.

Exercise 9.1.1. Fine the character table of $\mathbb{Z}/p\mathbb{Z} \rtimes_{id} (\mathbb{Z}/p\mathbb{Z})^\times$ for $p > 2$ prime.

9.2. **Monomial representations.** Consider a finite group G acting on a non-empty set S. Construct a vector space V with basis $\{e_s : s \in S\}$; we have $\dim(V) = \sharp S$. There is a natural representation

$$\rho\colon G \to \mathrm{GL}(V), \quad \rho(g)(e_s) = e_{g*s}.$$

Such representations are called **monomial**.

In fact, we have already seen at least two instances of this construction. When $S = G$, and G acts by left multiplication, we get $V = \mathbb{C}[G]$ and $\rho = \rho^{reg}$. When $G = S_n$, and $S = \{1,2,\dots,n\}$, we get $V = \mathbb{C}^n$ and $\rho = \rho^{std}$. As in these cases, it is easy to check that

$$\chi_\rho(g) = I(g) = \sharp \text{ fixed points of } g \text{ in } S.$$

Applying CFF and the projection formula, we get

$$\frac{1}{\sharp G}\sum_{g\in G}\chi_\rho(g) = \sharp \text{ orbits of } G \text{ in } S = \dim(V^G). \tag{10}$$

One way one may get such actions, is by choosing a subgroup $B < G$ and letting $S = G/B$, the set of left cosets of B in G (in fact, any set S on which G acts is a union of such examples). The representation is called the **coset representation**, which explains the name we have been using for the action of G on S throughout the course.

To make the situation even more specific, assume that

$$G = N \rtimes_{\phi} B.$$

Therefore, $G = NB, N \cap B = \{1\}$. Then,

$$G/B = \{nB : n \in N\}.$$

We check that $gnB = nB \Leftrightarrow g \in nBn^{-1}$. But,

$$nBn^{-1} = \{(n,1)(1,b)(n^{-1},1) : b \in B\} = \{(n\phi_b(n)^{-1}, b) : b \in B\}.$$

If $g = (n_1, b) \in nBn^{-1}$ it means that g necessarily equals to $(n\phi_b(n)^{-1}, b)$ for some n. We conclude that

$$\chi((n_1,b)) = I((n_1,b)) = \sharp\{n \in N : n_1 = n\phi_b(n)^{-1}\}.$$

Continuing with a general analysis will require making more assumptions on ϕ. Instead, let us take the case of $F_{20} = \mathbb{Z}/5\mathbb{Z} \rtimes_{id} (\mathbb{Z}/5\mathbb{Z})^{\times}$. Here, $n_1 = n\phi_b(n)^{-1}$ is written in additive notation and the condition is $n_1 = (1-b)n$. Now,

- if $b \neq 1$ there is a unique solution to the equation $n_1 = (1-b)n$.
- if $b = 1$ and $n_1 = 0$ there are 5 solutions to the equation $n_1 = (1-b)n$.
- if $b = 1$ and $n_1 \neq 0$ there are no solutions to the equation $n_1 = (1-b)n$.

We conclude that the character χ has the values $\chi(a_1) = 5, \chi(a_2) = 0, \chi(c_2) = \chi(c_3) = \chi(c_4) = 1$. Therefore,

$$\chi = \chi_4 + \chi_0,$$

and that tells us how the representation decomposes. Incidentally, note that the action of F_{20} on the 5 cosets of B gives us the inclusion $F_{20} \subset S_5$ we used before.

9.3. **A combinatorial application.** Let G be a finite group acting transitively on a finite non-empty set S. Let

$$G_0 = \{g \in G : g \text{ has no fixed point in } S\}.$$

G_0 is a subset of G, not a subgroup. We proved before (Proposition **??**) that if $\sharp X \geq 2$ then

$$\sharp G_0 \geq 1.$$

Theorem 9.3.1 (Cameron-Cohen)**.**

$$\sharp G_0 \geq \frac{\sharp G}{\sharp X}.$$

Proof. Let $I(g) = \chi(g)$ be the number of fixed points of g in S, where χ is the character of the monomial representation of G coming from S.

Compare the proof of the following lemma to the proof of Lemma **??**. It is really the same.

Lemma 9.3.2. *We have*

$$\frac{1}{\sharp G} \sum_{g \in G} \chi^2(g) \geq 2.$$

Proof. Consider the action of G on the set $S \times S$, $g(a,b) = (g(a), g(b))$. The class function χ^2 is the character of this representation and the dimension of the space of invariant vectors is $\frac{1}{\sharp G}\sum_{g\in G}\chi^2(g)$, which is equal to the number of orbits of G in $S \times S$ by Equation (10). To prove the lemma we only need to show that there is more than 1 orbit. And, indeed, one orbit is the diagonal $\{(s,s) : s \in S\}$ and, since $\|S\| \geq 2$, there must be at least one more orbit. □

Let $n = \sharp S$. Note that for $g \notin G_0$ we have $1 \leq \chi(g) \leq n$ and therefore

$$\frac{1}{\sharp G} \sum_{g \in G - G_0} (\chi(g) - 1)(\chi(g) - n) \leq 0.$$

Therefore,

$$\frac{1}{\sharp G} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) \leq \frac{1}{\sharp G} \sum_{g \in G_0} (\chi(g) - 1)(\chi(g) - n) = n \cdot \frac{\sharp G_0}{\sharp G}.$$

On the other hand,

$$\begin{aligned}\frac{1}{\sharp G} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) &= \frac{1}{\sharp G} \sum_{g \in G} \chi^2(g) - (n+1) \frac{1}{\sharp G} \sum_{g \in G} \chi(g) + \frac{1}{\sharp G} \sum_{g \in G} n \\ &\geq 2 - (n+1) + n = 1.\end{aligned}$$

Combining the two inequalities, the theorem follows. □

J.-P. Serre used this in proving the following theorem in number theory.

Theorem 9.3.3. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n. The density of prime numbers p (in the set of all primes) such that f has no root modulo p is at least $1/n$.*

Example 9.3.4. If we take the most simple non-trivial situation $f(x) = x^2 + 1$, the theorem states that for at least $1/2$ the primes f has no zero modulo p.

On the other hand, f has a zero modulo p if and only if -1 is a square modulo p. As -1 has order 2 modulo p (if $p > 2$), this happens if and only if there are elements of order 4 in $\mathbb{Z}/p\mathbb{Z}^\times$. Using that $\mathbb{Z}/p\mathbb{Z}^\times$ is a cyclic group of order $p - 1$ we see that this is the case if and only if $p \equiv 1 \pmod 4$. Thus, we conclude that the density of primes of the form $4k + 3$ is at least $\frac{1}{2}$.[3]

10. Introduction to Fourier analysis on finite groups.

In this section we are following the fantastic book by P. Diaconis, *"Group representations in probability and statistics"* and if you find the following sections interesting, I very much recommend reading it; you should have essentially all the prerequisite knowledge for reading much of the book. Before commencing, let us mention that the theory of Fourier transform for groups has many applications for other branches of science (computer science, chemistry, physics, electrical engineering), and even within mathematics to many branches besides probability and statistics.

10.1. **Convolution.**

Let G be a finite group. Let

$$C(G, \mathbb{C}) = \{f \colon G \to \mathbb{C}\},$$

be the vector space of complex-valued functions on G. It is of course just the vector space $\mathbb{C}[G]$ we used many times before. A function f defines an element $\sum_g f(g)[g]$ of $\mathbb{C}[G]$, and conversely. It has dimension $\sharp G$.

For $g \in G$ define the **delta function** $\delta_g \colon G \to \mathbb{C}$ by

$$\delta_g(x) = \begin{cases} 1, & g = x \\ 0, & \text{else.} \end{cases}$$

This function corresponds to $[g] \in \mathbb{C}[G]$. The collection $\{\delta_g : g \in G\}$ is a basis for $C(G, \mathbb{C})$.

[3] It is known to be precisely $1/2$.

We define the **convolution** of two functions $f, g \in C(G, \mathbb{C})$ as

$$(f * g)(x) = \sum_{s \in G} f(xs^{-1}) g(s).$$

Note that for a non-abelian group in general $f * g \neq g * f$. In fact, convolution is just the product in the ring $\mathbb{C}[G]$; if we write an element of $\mathbb{C}[G]$ as $\sum_g a_g [g]$, where $a_g \in \mathbb{C}$, then

$$(\sum_g a_g[g]) + (\sum_g b_g[g]) = \sum_g (a_g + b_g)[g], \qquad (\sum_g a_g[g])(\sum_g b_g[g]) = \sum_g (\sum_s a_{gs^{-1}} b_s)[g].$$

And so, it is clear that $C(G, \mathbb{C})$ is a ring under addition of functions and convolution, with identity element δ_1. For the same reason, the following two properties are evident, nonetheless we prove the first in the language of convolutions.

- $\delta_g * \delta_h = \delta_{gh}$.
- $f = \sum_g f(g) \delta_g$.

Indeed, $(\delta_g * \delta_h)(x) = \sum_{s \in G} \delta_g(xs^{-1}) \delta_h(s) = \delta_g(xh^{-1})$, which is a function that is everywhere zero except at $x = gh$ where it is 1. Thus, $\delta_g * \delta_h = \delta_{gh}$.

10.2. **The Fourier transform.** The **Fourier transform** $\hat{f}$ of a function $f \in C(G, \mathbb{C})$ is a function on representations (ρ, V) of G. It associate to a representation ρ the element

$$\hat{f}(\rho) = \sum_{s \in G} f(s) \rho(s) \in \mathrm{End}(V).$$

We will always assume that the representations are unitary, which we can always achieve by a suitable inner-product.

Lemma 10.2.1. *We have the following properties of the Fourier transform:*

(1) $\widehat{f+g} = \hat{f} + \hat{g}$, *and* $\widehat{\alpha f} = \alpha \hat{f}$, $\alpha \in \mathbb{C}$.
(2) $\hat{\delta}_g(\rho) = \rho(g)$.
(3) $\widehat{f * g} = \hat{f} \cdot \hat{g}$.
(4) Let U be the **uniform distribution** *on G, $U(g) = \frac{1}{|G|}, \forall g \in G$. Let (ρ, V) be a representation of G. Then $\hat{U}(\rho)$ is the projection operator on the sub-representation V^G. Thus, if ρ is irreducible and $\rho \not\cong \mathbb{1}$ then $\hat{U}(\rho) = 0$, while $\hat{U}(\rho)(\mathbb{1}) = 1$.*

Proof. The first two properties are immediate from the definition. For the third,

$$\begin{aligned}\widehat{f * g}(\rho) &= \sum_{s \in G} (\sum_{t \in G} f(st^{-1}) g(t)) \cdot \rho(s) \\ &= (\sum_{x \in G} f(x) \rho(x))(\sum_{t \in G} g(t) \rho(t)) \\ &= \hat{f}(\rho) \cdot \hat{g}(\rho).\end{aligned}$$

The fourth property is just the definition of the projection operator and the fact that V^G is a subrepresentation of V. □

10.3. **Fourier Inversion and Plancherel's formula.** The following theorem is very much reminiscent of Fourier analysis over $\mathbb{R}$.

Theorem 10.3.1. *Let $\rho_1, \dots, \rho_h$ be unitary representatives for the irreducible representations of G and let $d_i = \dim(\rho_i)$, $\chi_i = \chi_{\rho_i}$.*

(1) (Fourier Inversion). For any function $f \in C(G, \mathbb{C})$,

$$f(s) = \frac{1}{|G|} \sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1}) \hat{f}(\rho_i)). \tag{11}$$

(2) (Plancherel's formula) For any two functions $f, h \in C(G, \mathbb{C})$,

$$\sum_{s \in G} f(s^{-1}) h(s) = \frac{1}{|G|} \sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho_i) \hat{h}(\rho_i)). \tag{12}$$

Proof. The proof is surprisingly simple for such scary looking formulas. First note that by linearity and bilinearity, it is enough to prove Fourier inversion for the functions δ_g, and the Plancherel formula for the functions δ_g, δ_h. We first verify Fourier inversion for δ_g. In this case, the right hand side of (11) evaluated at s is:

$$\begin{aligned}
\frac{1}{|G|} \sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1}) \hat{\delta}_g(\rho_i)) &= \frac{1}{|G|} \sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1}) \rho_i(g)) \\
&= \frac{1}{|G|} \sum_{i=1}^{h} d_i \cdot \mathrm{Tr}(\rho_i(s^{-1} g)) \\
&= \frac{1}{|G|} \sum_{i=1}^{h} d_i \chi_i(s^{-1} g) \\
&= \frac{1}{|G|} \rho^{reg}(s^{-1} g).
\end{aligned}$$

This is a function that vanished everywhere, except at $s = g$, where it receives the value 1. Namely, this is just the function $\delta_g(s)$, as required.

The right-hand side of Plancherel's formula (12) is equal to

$$\begin{aligned}
\frac{1}{|G|} \sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{\delta}_g(\rho_i) \hat{\delta}_h(\rho_i)) &= \frac{1}{|G|} \sum_{i=1}^{h} d_i \mathrm{Tr}(\rho_i(g) \rho_i(h)) \\
&= \frac{1}{|G|} \sum_{i=1}^{h} d_i \mathrm{Tr}(\rho_i(gh)) \\
&= \frac{1}{|G|} \sum_{i=1}^{h} d_i \chi_i(gh) \\
&= \frac{1}{|G|} \rho^{reg}(gh).
\end{aligned}$$

This expression is equal to 1 if $g = h^{-1}$, and is equal to 0 otherwise. The sum

$$\sum_{s \in G} \delta_g(s^{-1}) \delta_h(s)$$

has exactly the same property, and we get the equality we were after. □

We now derive a variant of Plancherel's formula that is very useful for applications. Recall the (potentially confusing, but customary) notation for a complex matrix M: $M^* = \bar{M}^t$.

Corollary 10.3.2. *Let f be a real-valued function then*

$$\sum_{s\in G} f(s)h(s) = \frac{1}{|G|}\sum_{i=1}^{h} d_i \cdot \mathrm{Tr}((\hat{f}(\rho_i))^* \cdot \hat{h}(\rho_i)). \tag{13}$$

Proof. Let g be the function $g(s) = f(s^{-1})$. Then $\sum_{s\in G} f(s)h(s) = \sum_{s\in G} g(s^{-1})h(s)$ and we can apply Plancherel's formula to this sum. It only remains to note that for $\rho = \rho_i$ for some i,

$$\hat{g}(\rho) = \sum_s f(s^{-1})\rho(s) = \sum_s f(s)\rho(s^{-1}) = \sum_s f(s)\rho(s)^* = (\sum_s f(s)\rho(s))^* = \hat{f}(\rho)^*,$$

where we used that ρ_i is unitary and f is real-valued. □

10.4. **Random walks on cyclic groups.** Let p be a positive integer and consider the integers modulo p, $\mathbb{Z}/p\mathbb{Z}$. For various applications in cryptography, statistics, computer science and more, it is of interest to randomly choose a congruence class modulo p, or to emulate a random walk on $\mathbb{Z}/p\mathbb{Z}$. True randomness is hard; it's hard to generate and hard to "excavate" from nature. For that reason, one tries to expand, or stretch, a small amount of randomness to create a process that is pseudo-random; it is not completely random, but for all practical purposes, it is.

Consider then the following process

$$x_{k+1} = a_k x_k + b_k, \quad k = 1, 2, \dots.$$

At each iteration a_k and b_k can be chosen among the classes $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathbb{Z}/p\mathbb{Z}$, respectively, according to some agreed upon distribution. (This process is related to pseudo-random number generators, but we will now get into that here.) The simplest situation that is not completely deterministic is

$$a_k = 1, \forall k, \quad b_k \text{ chosen from } \{\pm 1\} \text{ with equal probability.}$$

This process just requires a fair coin-toss at every step.

Let us denote functions on $\mathbb{Z}/p\mathbb{Z}$ by vectors $(a_0, \dots, a_{p-1})$. And let us suppose that the initial seed is $x_0 = 0$, namely, it is the vector $(1, 0, \dots, 0)$ with probability 1. Then, the distribution after one iteration is $P = (0, 1/2, \dots, 1/2)$, and after n-steps it is given by $P^{*n} := P * P * \cdots * P$ (convolution n-times). For example, applying the random walk twice, it is clear that we can only end at $0, 2$ of $-2 = n-2$, and the probability we end at 0 can be found as

$$P(b_1 = 1)\cdot P(b_2 = -1) + P(b_1 = -1)\cdot P(b_2 = 1) = \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}.$$

Similarly the probability for ending at 2 is $P(b_1 = 1)\cdot P(b_2 = 1) = 1/4$, and so on. We recognize that we are just calculating $P * P$. For example, $P * P(0) = \sum_{j=0}^{p-1} P(j)P(-j) = P(1)P(p-1) + P(p-1)P(1) = 1/2$.

Let us switch for a moment to multiplicative notation (which will hopefully be less confusing), and write $\mathbb{Z}/p\mathbb{Z} = \langle t \rangle$ where $t^p = 1$. Using the group-ring presentation, we can say that

$$P = \frac{1}{2}(t + \frac{1}{t}),$$

and so

$$P^{*n} = \frac{1}{2^n}(t + \frac{1}{t})^n = \frac{1}{2^n}\sum_{j=0}^{n} a_j(n) t^j,$$

where

$$a_j(n) = \sum_{i\in\{0,\dots,n\}, 2i-n\equiv j(p)} \binom{n}{i}.$$

The limiting distribution is thus

$$\lim_{n \to \infty} P^{*n} = \lim_{n \to \infty} (a_0(n), a_1(n), \ldots, a_{p-1}(n)).$$

Our main interest is to know whether $\lim_{n \to \infty} P^{*n}$ approaches the uniform distribution U, and, if so, how fast? The fact that it approaches U is fairly easy (and follows from basic theory of Markov chains). The main question is how quickly it approaches U.

To gauge this we introduce the **total variation norm** $\| \cdot \|_{max}$. Let G be a finite group. For any two probability distributions $P, Q \in C(G, \mathbb{C})$ we let

$$\|P - Q\|_{max} = \max_{A \subset G} |P(A) - Q(A)| = \frac{1}{2} \sum_{g \in G} |P(g) - Q(g)|,$$

where $P(A) = \sum_{a \in A} P(a)$ is the probability of the event A.

Lemma 10.4.1 (Diaconis-Shahshahani). *Let G be a finite group with irreducible (unitary) representations $\rho_1 = \mathbb{1}, \ldots, \rho_h$. and let P be a probability distribution on G. Then,*

$$\|P - U\|_{max}^2 \leq \frac{1}{4} \sum_{i=2}^{h} d_i \cdot \mathrm{Tr}(\hat{P}(\rho_i)^* \cdot \hat{P}(\rho_i)).$$

(Namely, the trivial representation $\mathbb{1}$ is the only one not appearing in this sum.)

We will prove this lemma later on. Let us first see its application for the process we are discussing. In this case, recall that the irreducible representations of $\mathbb{Z}/p\mathbb{Z}$ are the 1-dimensional representations $\{\rho_j : j = 0, 1, \ldots, p-1\}$, where

$$\rho_j(a) = \zeta^{aj} \quad (\zeta = e^{2\pi i/p}).$$

(Namely, ρ_j is the character such that $\rho_j(1)$ is the p-th root of unity $e^{j2\pi i/p}$.) Then,

$$\hat{P}(\rho_j) = \frac{1}{2}(\rho_j(1) + \rho_j(-1)) = \cos(2\pi j/p).$$

By multiplicativity of the Fourier transform,

$$\hat{P}^{*n}(\rho_j) = \cos(2\pi j/p)^n.$$

Applying the Diaconis-Shahshahani lemma we find

$$\|P^{*n} - U\|_{max}^2 \leq \frac{1}{4} \sum_{j=1}^{p-1} \cos(2\pi j/p)^{2n}.$$

This last sum, though elementary in appearance, is not that easy to estimate, yet a relatively elementary argument gives a bound and one gets the following, if $p \geq 7$ and **odd**:

$$\|P^{*n} - U\|_{max}^2 \leq e^{-\frac{\pi^2}{2} \cdot \frac{n}{p^2}}.$$

This can be formulated qualitatively as saying that

"for $a_k \equiv 1$, and b_k chosen uniformly from the set $\{1, -1\}$, about p^2 iterations of the process

$$x_{k+1} = a + kx_k + b_k$$

are required to achieve a distribution close to the uniform distribution."

One can perform a similar analysis for the case $a_k = 1$ and b_k chosen uniformly from $\{0, 1, -1\}$ and get a very similar result. On the other hand, in stark-contrast, one can prove the following results for p such that $\gcd(p, 6) = 1$:

"for $a_k \equiv 3$, and b_k chosen uniformly from $\{1, -1\}$, about $\log p$ iterations of the process $x_{k+1} = a_k x_k + b_k$ are required to achieve a distribution close to the uniform distribution."

One reason the estimates are so different is that we are transferring from representation theory for the group $\mathbb{Z}/p\mathbb{Z}$ to representation theory for the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$. The process $x_{k+1} = 3x_k + b_k$ is thought of as coming from a random walk on the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$ corresponding to taking powers of the random element $(b, 3)$, where $b = \{1, 0, -1\}$ with equal probability. See Exercise 10.4.2

Exercise 10.4.2. Prove that last estimate using the Diaconis-Shahshahani lemma for the group $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}^\times$. (Finding the representations is Exercise 9.1.1.)

10.5. **Proof of the Diaconis-Shahshahani lemma.** Let us now prove the lemma. Recall the statement:

Let G be a finite group with irreducible (unitary) representations $\rho_1 = \mathbb{1}, \dots, \rho_h$. and let P be a probability distribution on G then

$$\|P - U\|^2_{max} \leq \frac{1}{4} \sum_{i=2}^{h} d_i \mathrm{Tr}(\hat{P}(\rho_i)^* \cdot \hat{P}(\rho_i)).$$

(Namely, the trivial representation $\mathbb{1}$ is the only one not appearing in this sum.)

Proof. Applying the Cauchy-Schwarts inequality for real numbers $(\sum a_n b_n)^2 \leq (\sum a_n^2)(\sum b_n^2)$ and taking all the $b_n = 1$, we find that

$$4\|P - U\|^2_{max} = (\sum_{s \in G} |(P(s) - U(s)|)^2 \leq \sharp G \cdot \sum_{s \in G} (P(s) - U(s))^2.$$

We view the last sum as $\sum_{s \in G} f(s)h(s)$, where $f(s) = h(s) = (P(s) - U(s))$. Apply the version of Plancherel's formula given in Corollary 10.3.2 to find

$$\sharp G \cdot \sum_{s \in G} (P(s) - U(s))^2 \leq \sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho)^* \cdot \hat{f}(\rho))$$

Now, $\hat{f}(\rho_i) = (\hat{P} - \hat{U})(\rho_i)$ and, using Lemma 10.2.1, we see that it is equal to $\hat{P}(\rho_i)$ for $\rho_i \neq \mathbb{1}$ (i.e., for $i > 1$), while $\hat{f}(\mathbb{1}) = (\hat{P} - \hat{U})(\mathbb{1}) = 1 - 1 = 0$. Therefore, we find

$$\sum_{i=1}^{h} d_i \mathrm{Tr}(\hat{f}(\rho)^* \cdot \hat{f}(\rho)) = \sum_{i=2}^{h} d_i \mathrm{Tr}(\hat{P}(\rho)^* \cdot \hat{P}(\rho)),$$

and the proof is complete. □

10.6. **Riffle shuffles.** This is a famous problem that one can attack by similar techniques. The actual estimates are very difficult though and, in any case, not accessible to us because they require full and detailed knowledge of the representation theory of the symmetric group. It is interesting, nonetheless, to see how the problem is set up and the first steps of the analysis.

A deck of cards, consisting of N cards ($N = 52$ in a usual deck) is split into two piles, one with k cards and the other with $N - k$ cards, with probability $\frac{1}{2^N}\binom{N}{k}$. Say, the left pile and the right pile. Then the cards from the two piles are interleaved randomly, where a card is chosen from the left pile with probability k/N and from the right pile with probability $(N - k)/N$. In the new pile the cards appear in a new order that is a permutation $\pi \in S_N$. Such a permutation is called, naturally enough, a **shuffle**, and the process of shuffling cards this way is called **riffle shuffle** or **dovetail shuffle**. It has the following form for some k

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & \dots & \dots & N-2 & N-1 & N \\ k+1 & 1 & 2 & k+2 & 3 & k+4 & \dots & k-2 & \dots & k-1 & N & k \end{pmatrix}$$

Experiments show that this is a good model for real-life card shuffles.

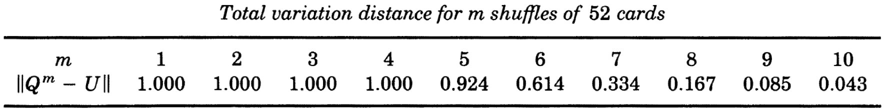
After n shuffles we get a certain probability distribution on S_N. If P is the original distribution, the distribution after n shuffles is P^{*n}. It is easy to understand the distribution P. We have $P(\pi) = 0$ if π is not a k-shuffle for any k, and $P(\pi) = 2^{-N}$ if π is a k-shuffle. But it is complicated to describe P^{*n} (and you can convince yourself of that by considering the case $n = 2$); more sophisticated methods are needed.

Similarly to the case of random walks on $\mathbb{Z}/p\mathbb{Z}$, routine arguments with Markov chains show that $P^{*n} \to U$ relative to the total variation norm. The question is how fast? Once more the main idea is to use the Diaconis-Shahshahani Lemma to get an estimate of the form

$$\|P^{*n} - U\|_{max}^2 \leq \frac{1}{4} \sum_{\rho \neq \mathbb{1}, \text{ irred.}} \dim(\rho) \cdot \mathrm{Tr}((\hat{P}(\rho)^*)^n \cdot (\hat{P}(\rho))^n),$$

where now ρ runs over all irreducible representations of S_n and that, on the other hand, even 5 shuffle will exhibit significant bias towards particular permuations.

The following table (their Q is our P) is taken from a paper of Bayer and Diaconis. It shows that 7 shuffles suffice to shuffle reasonably-well a deck of 52 cards.



Total variation distance for m shuffles of 52 cards

m	1	2	3	4	5	6	7	8	9	10
$\|Q^m - U\|$	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043

10.7. **Rubik's cube.** We have discussed Rubik's cube in §**??**. in particular, we introduced the notation U, D, F, B, L, R and the Cayley graph relative to the generators $U^i, D^i, F^i, B^i, L^i, R^i$, $i = 1, 2, 3$. There is a rational for using these redundant set of generators; in practice, the moves $U^2, U^3 = U^{-1}$, for example, take almost the same time as U.

In cube solving competitions, cube scramblers are used. These are computer programs that produce a position of the cube and a set of instructions of how to get to it that judges use to create the cube positions to be solved. Naturally, we wish to have all cube positions given to the participants "equally hard", and also "hard enough" so that undeserving achievements will not be recorded as world-records. One needs to find a method that produces such positions. The scramblers are choosing randomly generators to provide directions for creating the cube positions. However, we would like to guarantee that (with high probability) such sets of directions lead to equally hard positions that are also among the hardest possible.

The question of which position requires the most moves to solve was open for a long time and was finally settled by Rokicki et al. that determined this number to be 20. (This number is known as "God's number"; I don't personally like this terminology.) The following table is taken from a paper of Rokicki; the first column indicates the minimal number of moves required to solve a position and the last column indicates the number of cube positions requiring this number. We ignore the middle column; it relates to the method of analysis used in their paper.

d	Canonical sequences	Positions
0	1	1
1	18	18
2	243	243
3	3,240	3,240
4	43,254	43,239
5	577,368	574,908
6	7,706,988	7,618,438
7	102,876,480	100,803,036
8	1,373,243,544	1,332,343,288
9	18,330,699,168	17,596,479,795
10	244,686,773,808	232,248,063,316
11	3,266,193,870,720	3,063,288,809,012
12	43,598,688,377,184	40,374,425,656,248
13	581,975,750,199,168	531,653,418,284,628
14	7,768,485,393,179,328	6,989,320,578,825,358
15	103,697,388,221,736,960	91,365,146,187,124,313
16	1,384,201,395,738,071,424	≈1,100,000,000,000,000,000
17	18,476,969,736,848,122,368	≈12,000,000,000,000,000,000
18	246,639,261,965,462,754,048	≈29,000,000,000,000,000,000
19	3,292,256,598,848,819,251,200	≈1,500,000,000,000,000,000
20	43,946,585,901,564,160,587,264	≈300,000,000

We see that the bulk of the cube positions require 18 moves. It is thus natural to perform the random process P and hope that P^{*n} is very closed to a distribution Q that has values, say, $Q(17) \approx Q(19) \approx 0.05$, $Q(18) \approx 0.90$ and otherwise $Q(i) \approx 0$. But, is it possible?? More precisely, what is

$$\min_n \|P^{*n} - Q\|_{max}.$$

I don't know the answer to that. (A careful analysis might require understanding the representations of the Cube group.) In real-life, the Tnoodle scrambler program is used by the World Cube Association to generate positions and the quality bar seems pretty low. At some point in time, they were OK with producing cube positions only guaranteed to require 11 moves or more, which seems rather bad. By simply running the program for say 1,000 times for each $n = 15 - 25$ and using fast cube-solvers, one could get a very reliable statistics on this question. The whole project shouldn't take more than a week to run a desktop computer.

11. Some of the applications of group representations

This is a very sketchy section that mainly contains pointers to the literature. I will leave it to you to chase these references down, if you are interested. First, there are the two survey articles by T. Y. Lam, *"Representations of Finite Groups: A Hundred Years, Part I, and Part II"*. You can find the articles here:

http://www.ams.org/notices/199803/lam.pdf
http://www.ams.org/notices/199804/lam2.pdf

Secondly, there is the following post on Math overflow about "Fun applications of representations of finite groups", from which I have learned a lot myself.

https://mathoverflow.net/questions/11784/fun-applications-of-representations-of-finite-groups

I don't know if I would have used the adjective "fun", but there are certainly diverse and interesting applications. You would note in particular applications to:

(1) *Chemistry and Physics*, specifically quantum chemistry and quantum physics. For example, one user mentions "The symmetry group of a molecule controls its vibrational spectrum, as observed by IR spectrosocopy. When Kroto et al. discovered C60, they used this method to demonstrate its icosahedral symmetry." They suggest *Group Theory and Chemistry* by David M. Bishop as a reference. Another post suggests the book *Group Theory and Physics* by S. Sternberg for the connections to Physics quoting Sternberg saying that "molecular spectroscopy is an application of Schur's lemma". Another very convincing book is *Group theory and its applications to physical problems* by M. Hamermesh.
(2) *Combinatorics*. A lot of this is done through representations of the symmetric group and related groups. This is a topic to which many books, book chapters, and articles are devoted. The symmetric group plays a crucial role in combinatorics, of course. Mathscinet returns 455 references for searching for "Representation" and "symmetric group" in title, among which 14 are books.
(3) *Probability and Statistics*. Here perhaps we can rest our case by referring to a book by one of the leading statisticians and probablists of our time *Group representations in probability and statistics* by P. Diaconis.
(4) Within *algebra*, the celebrated Feit-Thompson theorem uses the following theorem of Frobenius, to which the only known proofs use representation theory.

A finite group G is called a **Frobenius group** with Frobenius kernel K and Frobenius complement H if G has a subgroup H, such that for any $g \notin H$ we have

$$H \cap gHg^{-1} = \{1\}.$$

One lets in this case

$$K = \{1\} \cup (G - \bigcup_{g \in G} gHg^{-1}).$$

K is called the Frobenius kernel.

An example of a Frobenius group is the group of affine linear transformations of the line $\{ax + b\}$ with H being the linear transformations $\{ax\}$. We can also write this group as $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\}$.

Theorem 1 (Frobenius' theorem) *Let G be a Frobenius group with Frobenius complement H and Frobenius kernel K. Then K is a normal subgroup of G, and G is the semidirect product $K \rtimes H$.*

The hard part is to show that K is a group!

Theorem 2 (Frobenius' theorem, equivalent version) *Let G be a group of permutations acting transitively on a finite set X, with the property that any non-identity permutation in G fixes at most one point in X. Then the set of permutations in G that fix no points in X, together with the identity, is closed under composition.*

Apparently, there is still no proof of these theorems that avoids using group representations in an essential way. Although, recently, Terrence Tao gave a proof that only uses character theory for finite groups. I have learned much about this from reading Tao's blog

https://terrytao.wordpress.com/2013/04/12/the-theorems-of-frobenius-and-suzuki-on-finite-groups/

Another very nice application within Algebra is the proof of Burnside's theorem already cited: *if p, q are primes then a group of order $p^a q^b$ is solvable.* The proof is almost within our reach, but not quite. It uses several ideas from algebra that we hadn't discussed at all (such as the theory of modules and algebraic integers) and a little more than we had done regarding representations of groups. In particular, it uses an additional orthogonality relation: *the columns of the character table are orthogonal* in the following sense. Let G be a finite group and $g, h \in G$ elements. Let χ_i be the irreducible characters of G (that is, the characters of its irreducible representations) then:

$$\sum_{\chi_i} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |Cent_G(g)|, & \text{if } g, h \text{ are conjugate} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

(The summation extending over the irreducible characters.) The main idea here is the the rows are "essentially" a collection of orthonormal basis. Thus, if properly modified, one can make them into truly orthogonal matrix. That is, into a matrix M that satisfies $MM^* = I_h$ ($h = h(G)$). But then also $M^*M = I_h$ and reading this information carefully gives the orthogonality of the columns.

Finally, but still within the realm of pure Algebra, group representations have a lot to do with the study of simple groups. The classification of simple groups puts them in large families ($\mathbb{Z}/p\mathbb{Z}, A_n, \mathrm{PSL}_n(\mathbb{F}), \dots,$) but some escape this classification and fall into a category of themselves: the sporadic simple groups. There are finitely many such groups (27, in fact). The largest simple group is the Monster group, its order is

$$808, 017, 424, 794, 512, 875, 886, 459, 904, 961, 710, 757, 005, 754, 368, 000, 000, 000.$$

Its existence is a non-trivial fact. Before constructing the Monster, mathematicians suspected its existence and in fact predicted the dimensions of some of its smallest irreducible representations as 1, 196883 and 21296876, and were able, more generally, to work out its character table. John McKay, of Concordia university, made the audacious observation that those numbers are related to Fourier coefficients of the j-function, a function appearing in the theory of elliptic curves, which is part of number theory. Following that, precise conjectures were made by Conway and Norton, going under the name of "Moonshine".

Some of the key aspects of these conjectures were proven by R. Borcherds, a work that got him the Fields prize in 1998.

12. WHAT IS MISSING

We have barely scratched the surface when it comes to group representations. But, I would say that at the very basic entry level to representations of finite groups there is one more topic that we could have discussed if we had more time. This is the subject of **induced representations** and **Frobenius reciprocity**. Besides it's theoretical importance it is a powerful computational tool. This subject is completely within reach and those wishing to have a more complete picture are encouraged to pursue it using any textbook dealing with group representations.

Besides this topic, other glaring omissions are (i) tensor products of representation and their decomposition; some study of (ii) the representations of symmetric group and their connections to Young tableaux, hook lengths and other mysterious terminology; (iii) Representations of nilpotent groups, and in particular p-groups (Blichfeldt's theorem). Once more, these topics would (or should) be covered in most textbooks dealing with representations of finite groups; (iv) Representations of finite matrix groups, for example $\mathrm{GL}_n(\mathbb{F}_p)$.

Blichfeldt's theorem asserts that every irreducible representation of a finite nilpotent group G, for example, every irreducible representation of a finite p-group, is induced from a 1-dimensional representation of a subgroup H of G.

Going perhaps further back, some topics that should be covered in more detail as part of an introduction to finite groups are the topics: (i) Free groups and free products and the **Nielsen-Schreier theorem**; (ii) **Nilpotent groups** and the notions of **ascending** and **descending central series**. (iii) Simplicity of the groups $\mathrm{PSL}_n(\mathbb{F}_q)$. Once more, these topics are certainly accessible and it is only for reasons of time that we have omitted them.

Index